CENTRE HOSPITALIER Carcassonne

CHARTE DE SECURITE DE L'INFORMATION DU CENTRE HOSPITALIER DE CARCASSONNE

Version 5 du 16/12/2020

SUIVI DES MODIFICATIONS

VERSION	DATE	NATURE DE LA MODIFICATION
4	12/03/2015	Mise en conformité de la charte en regard des prérequis du programme Hôpital Numérique. Validation par la Direction Générale, la Commission médicale de l'Etablissement et la Commission Technique d'Etablissement.
5	16/12/2020	Mise en conformité de la charte en regard des prérequis RGPD

CENTRE HOSPITALIER Carcassonne	Charte de sécurité de l'information	
SIH_DOC_001	**Document**	**Version :2**
		Date d'application : 29/12/2021

SOMMAIRE

1. OBJET DU DOCUMENT 3

2. CHAMP D'APPLICATION ET PROCEDURES DE DIFFUSION 3
2.1 Personnel de l'établissement 4
2.2 Accès par des tiers aux systèmes d'information du CH 4
2.2.1. Fournisseurs titulaires d'un marché 5
2.2.2. Fournisseurs hors marché 5

3. DEFINITIONS 5

4. CADRE RÉGLEMENTAIRE 5

5. CRITÈRES FONDAMENTAUX DE LA SÉCURITÉ 6
5.1. Principes 6
5.2. Une mission sécurité 7
5.3. Un enjeu technique et organisationnel 7
5.4. Une gestion des risques 7

6. RÈGLES DE SÉCURITÉ 7
6.1. Accès au SIH 7
6.2. Confidentialité de l'information et obligation de discrétion 8
6.3. Protection de l'information 9
6.4. Usage des ressources informatiques 9
6.5. Usage des outils de communication 10
6.5.1 Usage du téléphone et du fax 10
6.5.2 Usage d'Internet / Intranet 10
6.5.3 Usage de La messagerie électronique : 11
6.5.4 Accès au SIH en dehors de l'établissement 12
6.6 Usage des logins et des mots de passe (ou de cartes CPS ou équivalent) 12
6.7. Droits et devoirs des administrateurs des systèmes informatiques 13
6.7.1. Missions des administrateurs 13
6.7.2. Disponibilité des données et du système informatique 13
6.7.3. Confidentialité des données 13
6.7.4. Contrôle de l'utilisation du système informatique 13
6.7.5. Accès à distance 13
6.8. Sécurité physique des bâtiments 13
6.9. Image de marque de l'établissement 14

7. PROTECTION DES DONNÉES A CARACTERE PERSONNEL 14
7.1. Droits des utilisateurs 14
7.2. Devoirs des utilisateurs 15

8. SURVEILLANCE DU SYSTÈME D'INFORMATION 16
8.1. Contrôle 16
8.2. Traçabilité 16
8.3. Alertes 16

9. RESPONSABILITÉS ET SANCTIONS 17

1. OBJET DU DOCUMENT

Le Centre Hospitalier de Carcassonne met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des équipements informatiques fixes et mobiles.

Les salariés, dans l'exercice de leurs fonctions, sont conduits à accéder et à utiliser lesdits équipements informatiques, ainsi que les systèmes d'information et de communication mis à leur disposition.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Par ailleurs, des tiers au Centre Hospitalier de Carcassonne (salariés suivis, prestataires externes, partenaires…) peuvent également avoir accès aux équipements informatiques et aux systèmes d'information et de communication du CH.

Cette charte a pour objectifs :

- de sensibiliser les utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer ;
- d'informer les utilisateurs sur :
  - les usages permis des moyens informatiques mis à sa disposition ;
  - les règles de sécurité en vigueur ;
  - les mesures de contrôle prises par le Centre Hospitalier de Carcassonne ;
  - les sanctions éventuellement encourues par les utilisateurs ;
- de formaliser les règles générales de sécurité que les utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques, et ainsi de déterminer les droits et devoirs des utilisateurs.

Ces règles s'inscrivent dans une démarche responsable afin de protéger d'une part le patrimoine informationnel et l'image de marque du Centre Hospitalier de Carcassonne, et d'autre part les libertés et la vie privée des personnes concernées que sont les salariés du Centre Hospitalier et les tiers en lien avec le Centre Hospitalier (salariés suivis, prestataires externes, partenaires…).

Le Responsable des systèmes d'information (RSI) ou le Directeur des systèmes d'information (DSI), la Direction Générale (DG) et le Délégué à la protection des données personnelles (DPD) ou le DPO (Data Protection Officer) se tiennent à la disposition des utilisateurs qui souhaiteraient disposer d'informations ou de conseils complémentaires relatifs à l'usage des systèmes d'information et des équipements informatiques.

Cette Charte a été validée par la Direction générale de l'établissement. Préalablement, elle a été notifiée à sa mise en œuvre à la Commission Médicale d'Etablissement. Elle constitue une annexe au Règlement Intérieur de l'établissement et est juridiquement opposable aux utilisateurs qui sont invités à en prendre connaissance. La Charte est mise à leur disposition sur l'Intranet et affichée dans les locaux de l'établissement de santé.

2. CHAMP D'APPLICATION ET PROCEDURES DE DIFFUSION

La présente charte concerne l'ensemble des moyens informatiques et de communication électronique qui sont mis à la disposition des utilisateurs à des fins professionnelles exclusivement, ainsi que l'ensemble des moyens informatiques et de communication électronique qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité professionnelle.
Les systèmes d'information et de communication du Centre Hospitalier sont notamment constitués des éléments suivants :

- ordinateurs portables ou fixes,
- ordinateurs de bureau et terminaux (clients légers),
- Terminaux Multimédia (TMM)
- périphériques (y compris clés USB),
- réseaux informatiques (serveurs, routeurs, connecteurs, bornes WIFI),
- photocopieurs,
- télécopieurs,
- téléphones (fixes et portables) et smartphones,
- tablettes électroniques,
- logiciels,
- fichiers informatiques et bases de données,
- espaces de stockage individuel,
- messagerie,
- connexions internet, intranet, extranet.

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 ou à partir du réseau administré par l'établissement. Toute demande de dérogation aux différents éléments définis dans le cadre de la présente Charte doit être présentée par écrit au responsable des systèmes d'information (RSI). La décision finale est ensuite prise en concertation avec la direction générale qui se réserve le droit d'accepter ou de refuser les demandes de dérogation.

Les procédures de diffusion et d'acceptation de la présente charte sont les suivantes :

2.1. Personnel de l'établissement

L'acceptation de la charte est réalisée :

- lors de l'arrivée du personnel dans l'établissement et de son passage par les services des ressources humaines ou des affaires médicales ;
- la remise en main propre de la charte à chaque agent ;
- et par la signature par chaque agent d'une attestation de prise de connaissance de cette charte.

Pour les anciens agents n'ayant pas signé d'attestation, une note d'information a été publiée sur l'Intranet et communiquée par courriel à tous les agents. Cette note d'information informe de l'existence de cette charte et une recommandation forte pour en prendre connaissance.
A chaque mise à jour de la charte, une note d'information est publiée sur l'Intranet et les agents en sont tous informés par courriel.

2.2. Accès par des tiers aux systèmes d'information du Centre Hospitalier

Tout utilisateur extérieur au Centre Hospitalier ne peut avoir accès aux systèmes d'information de l'établissement que moyennant une autorisation expresse préalable délivrée par le RSI et s'engage, dès lors, à respecter l'ensemble des dispositions de la présente charte.

2.2.1. Fournisseurs titulaires d'un marché

Pour chaque marché publié la charte est communiquée en annexe du CCTP avec les mentions suivantes :
- « Le titulaire s'engage à respecter la charte informatique annexée au présent CCTP… »
- « Le personnel des fournisseurs n'a pas obligation de signer la charte. Chaque titulaire est tenu responsable d'avoir transmis à son personnel la présente charte et des agissements de son personnel. »

Pour les marchés en cours d'exécution, une note d'information a été transmise à tous les responsables des titulaires les avertissant de l'existence de l'acceptation implicite de cette dernière sans préavis ni réserve spécifique.
A chaque mise à jour de la charte, une note d'information avec la charte en pièce jointe est transmise par courriel à chaque titulaire de marché en cours d'exécution.

2.2.2. Fournisseurs hors marché

Les fournisseurs traités hors marché font l'objet d'un traitement au cas par cas compte tenu du faible nombre de fournisseurs ayant un accès au SIH et donc concerné par la présente charte. Le processus mis en place consiste donc pour le responsable de ces fournisseurs à solliciter le RSSI si un accès au SIH est réalisé.
Pour les fournisseurs en cours, un inventaire a été réalisé en date de rédaction de la présente charte en version 5, et aucune attestation n'a été requise.

3. DEFINITIONS

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

- Système d'Information Hospitalier (SIH) : ensemble constitué d'ordinateurs, de serveurs, de réseaux interconnectés, de logiciels, de données immatérielles, de périphériques nécessaires, ainsi que l'organisation, les processus et les ressources associées pour assurer son maintien en condition opérationnel.
- 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, forum, etc.).
- Utilisateurs : les personnes (internes ou externes) ayant accès ou utilisant les ressources informatiques et les services internet de l'établissement.
- Administrateur : toute personne qui administre les serveurs et les machines dépendantes directement du service informatique ainsi que les personnes habilitées par le service.

4. CADRE RÉGLEMENTAIRE

Le cadre réglementaire de la sécurité de l'information est présenté dans la PGSSI (cf. chapitre 2.1. Cadre Juridique). Néanmoins, les grands thèmes sont les 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.

D'une façon générale, 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 ;
- du secret professionnel qui est général et absolu. La mort du malade ne délivre ni le médecin, ni aucun membre du personnel de cette obligation.

« Le secret professionnel, institué dans l'intérêt des malades, s'impose à tout membre du personnel du centre hospitalier quel que soit son métier, son grade, qu'il soit soignant ou non. Le secret couvre tout ce qui est venu à la connaissance du personnel dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris »

5. CRITÈRES FONDAMENTAUX DE LA SÉCURITÉ

5.1. 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, …), sur les personnels (paie, gestion du temps, évaluations, accès à Internet et à la messagerie, …), et la comptabilité.

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, ...

Du fait de la collecte de données et du traitement de celles-ci réalisés, le CH s'engage, dans le cadre des dispositions légales et réglementaires qui s'imposent à lui et dans le respect du principe de proportionnalité édicté par le RGPD, à mettre en œuvre toutes les mesures organisationnelles et techniques utiles afin de préserver la sécurité, l'intégrité et la confidentialité des Données, ainsi que la sécurité de son système d'information et de communication, sur le plan technologique et procédural, afin notamment d'empêcher toute modification, tout transfert et toute suppression non-autorisés des Données, et toute intrusion non-autorisée dans son système d'information ou son endommagement.

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.

5.2. Une mission sécurité

Le Centre Hospitalier de Carcassonne fournit un système d'information qui s'appuie sur une infrastructure informatique. Elle doit assurer la mise en sécurité de l'ensemble 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.

5.3. 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 de Carcassonne 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. Toutefois, le premier risque reste le risque humain lié aux traitements et aux manipulations des Données par les Utilisateurs, et par l'utilisation par ces derniers du système d'information et de communication et des outils qui y sont liés.

Par conséquent, la mise en place d'outils de sécurité ne doit pas dispenser les utilisateurs de signaler toute tentative d'intrusion extérieure, de falsification ou de présence de virus au responsable des systèmes d'information.

Tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des moyens mis à sa disposition et du réseau auquel il a accès, principalement en évitant l'intrusion de virus susceptibles d'endommager le système d'information de l'établissement.

5.4. Une gestion des risques

L'information médicale et comptable, qu'elle soit numérique ou non, est un composant sensible qui intervient dans tous les processus de prise en charge des patients et de gestion globale de l'établissement. 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, …) et des impacts financiers (recettes en baisse, détournements de fonds, …). De même, la sécurité repose sur une gestion des risques avec des analyses de risques potentiels, de suivis d'incidents, de dispositifs d'alertes. La communication vers les utilisateurs est un volet important de cette gestion. La présente Charte s'inscrit dans ce plan de communication.

6. RÈGLES DE SÉCURITÉ.

6.1. Accès au SIH

L'accès à la totalité du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe). Une demande préalable écrite est ainsi requise pour l'attribution d'un accès aux ressources informatiques.

Chaque utilisateur reçoit un droit d'accès individuel qui se matérialise par un code utilisateur un mot de passe, un badge ou carte.
Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'accès des utilisateurs. Ils ne doivent être communiqués à personne, ni responsable hiérarchique, ni informatique. Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Chaque utilisateur doit s'identifier personnellement et ne peut utiliser l'identité d'autrui (même avec l'accord de ce dernier).

Ce droit d'accès cesse automatiquement 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.

6.2. Confidentialité de l'information et obligation de discrétion

Les personnels de l'établissement sont soumis au secret professionnel et 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.

Article 226-13 (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002) :

La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux propres à l'utilisateur, publics ou partagés, dans un cadre strict ou réglementé (à titre d'exemple, les données médicales ne sont accessibles qu'aux personnes habilitées et ceux dans le cadre de la prise en charge des patients). 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 courriers électroniques 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 s'effectue par simple login et mot de passe. Conformément au cadre réglementaire, l'usage de la carte CPS et CPE sera prochainement généralisé pour l'accès aux données de santé.

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, des informations nominatives et/ ou confidentielles couvertes par le secret professionnel.

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 regarder, modifier ou détruire des informations appartenant à d'autres utilisateurs sans leur autorisation ;
- de perturber le bon fonctionnement des systèmes informatiques et du réseau que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels non autorisés ou parasites connus sous le nom générique de virus ;
- de rendre accessible à des tiers des données et informations confidentielles pour lesquelles ils n'ont pas d'autorisation ;
- de se connecter ou d'essayer de se connecter sur un serveur sans y avoir été autorisé par les responsables habilités.

6.3. 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 est important 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 hébergés dans des salles protégées. De même, les documents bureautiques produits doivent être 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, ceux qui utilisent un matériel portable (exemples : poste, tablette, smart phone, …) ne doivent pas le mettre en évidence pendant un déplacement, ni exposer son contenu à la vue d'un voisin de train … ; le matériel doit être rangé en lieu sûr. De même, il faut ranger systématiquement en lieu sûr tout support mobile de données (exemples : CD, disquette, clé, disque dur, …). 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 médias de stockage amovibles (exemples : clefs USB, CD-ROM, disques durs …) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants (virus) 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. Des procédures sont prévues à cet effet.
D'une manière générale, l'information ne peut être communiquée qu'aux personnes dument habilitées à la recevoir.

6.4. 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 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).

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

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.

Les utilisateurs doivent périodiquement effectuer des sauvegardes de leurs données, ou de façon préférable, il leur est conseillé de travailler directement sur un serveur sur lequel leur sera alloué un répertoire de travail dont le contenu sera sauvegardé quotidiennement.

Un utilisateur ne devra jamais quitter son poste de travail sans se déconnecter ou verrouiller sa session.

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

L'usage de matériel personnel (tablette, smartphone, …) connecté au SIH doit en préalable faire l'objet d'une autorisation du Service Informatique pour identifier le plus clairement possible les actions autorisées ou non et ainsi organiser sur mesure l'utilisation du matériel numérique personnel par l'agent dans l'exercice de ses fonctions, comme par exemple :

- Imposer des conditions de sécurités au salarié (antivirus, protection matérielle des terminaux contre le vol…) ;
- Désigner la propriété des données professionnelles contenues dans l'interface personnelle (au cours de l'exécution du contrat de travail et à son terme.) ;
- Etablir précisément ce qui relève de la vie personnelle ou de la vie professionnelle du salarié ;
- Préciser les modalités de contrôle et les sanctions encourues…

6.5. 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.

6.5.1. 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.

6.5.2. Usage d'Internet / Intranet

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, aux bonnes mœurs ou à l'image de marque de l'établissement, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information du Centre Hospitalier ou engageant financièrement celle-ci.

Tous les accès Internet sont tracés et enregistrés et conservés par un dispositif de filtrage et de traçabilité. Ces dispositifs font l'objet d'une déclaration auprès de la CNIL. La finalité de l'usage de ces dispositifs de journalisation n'est pas de pas porter atteinte au droit au respect de la vie privée des utilisateurs, mais plus à des fin d'investigation en cas d'incident de sécurité grave et avéré.

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 RSI, pour des raisons de sécurité, peut limiter ou prohiber l'accès à certains sites. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

6.5.3. Usage de La messagerie électronique

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

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les utilisateurs sont invités à informer la direction informatique des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

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, valoir offre ou acceptation de manière à former un contrat entre l'hôpital et son interlocuteur.
L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale du Centre Hospitalier et/ou de l'utilisateur.
Tout message envoyé ou reçu depuis votre messagerie professionnelle est supposé avoir un caractère professionnel, sauf s'il est clairement identifié comme étant personnel (avec l'indication « Personnel » ou « Privé » en objet) ou classé dans un répertoire « Personnel ».
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 provocantes 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. Seules les pièces jointes professionnelles de type « documents » ou « images » sont autorisées. 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 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.

Lors de son départ de l'établissement, l'utilisateur doit respecter la procédure de départ et remettre l'ensemble des moyens informatiques et de communication électronique qui lui ont été remis (ordinateur, périphériques, mobile, carte d'accès, moyen d'authentification à distance, badges, supports de stockage, etc.) en bon état général de fonctionnement et ne

conserver aucun matériel ou aucune donnée permettant d'accéder au système d'information. De plus, l'utilisateur s'interdit, avant son départ, de détruire des informations et des données professionnelles.

6.5.4. Accès au SIH en dehors de l'établissement

Le présent article concerne l'accès et l'utilisation des systèmes d'information du Centre Hospitalier, de ses ressources, et des moyens de communication par l'utilisateur lorsque celui-ci est situé en-dehors du site physique de l'établissement.

L'ensemble des dispositions de la présente charte sont applicables aux utilisateurs accédant aux systèmes d'information et de communication du Centre Hospitalier à distance.

6.6. Usage des logins et des mots de passe (ou de cartes CPS ou équivalent)

Chaque utilisateur dispose de 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, soit d'une carte CPS ou équivalent (avec un code personnel à 4 chiffres)

Le mot de passe choisi doit être robuste (8 caractères minimum, mélange de chiffres, lettres et caractères spéciaux), de préférence simple à mémoriser, mais surtout complexe à deviner. Il doit 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.

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

6.7. Droits et devoirs des administrateurs des systèmes informatiques

6.7.1. Missions des administrateurs

L'administrateur système est responsable de la qualité de service du système informatique mis à la disposition des utilisateurs. Il doit en outre s'attacher à faire respecter les droits et les devoirs des utilisateurs.

6.7.2. Disponibilité des données et du système informatique

Dans ce cadre et à titre non exhaustif, l'administrateur a notamment pour tâches :

- d'effectuer les sauvegardes des données des serveurs, qui doivent rendre possible la restauration des données détruites par erreur ;
- de minimiser les périodes d'indisponibilité du service, et faire en sorte qu'elles soient le moins pénalisantes possible pour les utilisateurs ;
- d'informer à l'avance les utilisateurs des interruptions de service planifiées.

6.7.3. Confidentialité des données

La consultation des fichiers des utilisateurs par l'administrateur ne peut s'effectuer que dans le respect des règles de confidentialité applicables aux données contenues dans les fichiers. De même, les administrateurs ont l'obligation de préserver et de respecter la confidentialité des informations qu'ils sont amenés à connaître dans le cadre de leur activité.

6.7.4. Contrôle de l'utilisation du système informatique

A titre non exhaustif, et pour permettre d'assurer la qualité de service du système informatique et le respect par les utilisateurs des règles définies à la présente Charte, l'administrateur se voit notamment investi des pouvoirs :

- de surveiller les sessions des utilisateurs ;
- de modifier la priorité, ou supprimer (avec préavis) les tâches qui consomment trop de ressources ;
- de compresser les fichiers trop volumineux (à l'exception des dossiers personnels) ou les supprimer avec préavis.

6.7.5. Accès à distance

Dans le cadre d'opération de maintenance, les administrateurs sont habilités à prendre la main à distance sur les postes de travail de l'hôpital.

6.8. SÉCURITÉ PHYSIQUE DES BÂTIMENTS

L'accès aux bâtiments et aux zones internes doit s'effectuer selon des dispositifs cohérents au regard de la criticité des informations stockées ou traitées. Par défaut, l'accès aux zones par un tiers doit s'effectuer accompagné par un personnel du Centre Hospitalier, les portes d'accès aux zones sensibles doivent rester fermées.
Toute anomalie ou incident constaté doit être signalé :

- au personnel d'encadrement, notamment en cas de constat d'une utilisation à son insu ;
- au support utilisateurs du service informatique, afin que tout soit mis en œuvre pour traiter l'incident.

6.9. IMAGE DE MARQUE DE L'ÉTABLISSEMENT

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.

7. PROTECTION DES DONNÉES A CARATERES PERSONNEL

7.1 Droits des utilisateurs

Le centre hospitalier met en œuvre des traitements de données à caractère personnel en relation avec l'usage et la sécurité des systèmes d'information et de communication couverts par la présente charte. L'établissement s'engage à ce que les données concernant les utilisateurs soient collectées et traitées de manière loyale et licite, dans les conditions exposées.

L'établissement a désigné un Délégué à la protection des données joignable à l'adresse dpo@ch-carcassonne.fr.

Les catégories suivantes de données sont traitées :

- Informations professionnelles
- Informations relatives à l'identité
- Coordonnées professionnelles
- Log de connexion et autre trace informatique
- Informations sur l'utilisation des systèmes d'information et de communication

Ces catégories de données proviennent essentiellement des systèmes d'information et de communication ainsi que des annuaires informatiques et des directions des ressources humaines.

Ces données sont conservées selon les durées légales.

Ces données sont destinées à l'établissement ainsi qu'aux personnes habilitées au sein de l'établissement et aux autorités habilitées.
Les traitements opérés dans le cadre de la charte ont pour finalité :

- le suivi et la maintenance des systèmes d'information et de communication, qu'il s'agisse des applications informatiques internes ou des accès vers l'extérieur (soit notamment l'accès à internet) ;
- la gestion des annuaires et référentiels permettant de définir les autorisations d'accès aux applications et réseaux ;
- la mise en œuvre de dispositifs destinés à assurer la sécurité et le bon fonctionnement des systèmes d'information et de communication, notamment la conservation des logs de connexion, des traces informatiques et des données de toute nature, conformément à la Politique de gestion des journaux informatisés (PGJI) notamment à des fins d'historisation et de preuve de l'utilisation des systèmes d'information et de communication ;
- la gestion de la messagerie électronique ;
- le fonctionnement en réseaux internes par métiers ou par projet permettant la collecte, la diffusion ou la traçabilité de données de gestion des tâches, de la documentation, de la gestion administrative et des agendas des personnes répertoriées dans ces réseaux ;
- le contrôle du respect de la charte et les audits de sécurité ;
- les statistiques, investigations et enquêtes

Ces finalités permettent au Centre Hospitalier de poursuivre des intérêts légitimes liés à la bonne utilisation et à la sécurité de ses systèmes d'information et de communication dans le respect des droits des utilisateurs.

A toutes fins utiles, il est rappelé que les données collectées auprès des utilisateurs sont obligatoires aux fins de bonne gestion, d'organisation et de sécurité des systèmes d'information et de communication.
Conformément à la loi « Informatique et libertés », les utilisateurs sont informés, en particulier, qu'ils disposent d'un droit :

- d'interrogation,
- d'accès,
- de limitation,
- d'effacement,
- de rectification,
- d'opposition,

au traitement des données les concernant et qui s'exerce auprès du Délégué à la protection des données (dpo@ch-carcassonne.fr). Par ailleurs, les utilisateurs disposent d'un droit de réclamation auprès de la Cnil.
Les personnes concernées peuvent également donner des directives relatives à la conservation, à l'effacement et à la communication de leurs données après leur décès.
Une personne peut être désignée pour exécuter ces directives et elle aura alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. Lorsqu'il s'agit de directives particulières, elles peuvent également être confiées aux responsables de traitement en cas de décès.
Afin d'assurer la confidentialité des données à caractère personnel qu'ils traitent, les Utilisateurs s'interdisent d'en faire part à des services non habilités à en prendre connaissance. Également, tout Utilisateur s'interdit de prendre connaissance des données qui ne lui sont pas destinées ou dont il n'est pas habilité à prendre connaissance. De la même façon, il est interdit de communiquer par quelque moyen que ce soit à des tiers non autorisés des données à caractère personnel traitées pour le compte du Centre Hospitalier. En cas de doute, l'Utilisateur doit demander l'avis du DPO préalablement à la transmission des données.

En tout état de cause, il est nécessaire d'informer le Délégué à la Protection des Données dans les meilleurs délais de tout risque présumé pour la sécurité des données à caractère personnel.

Tout Utilisateur qui contreviendrait à ces obligations peut engager la responsabilité personnelle et peut être passible de sanctions telles que prévues dans le règlement intérieur.

7.2 Devoirs des utilisateurs

Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel, prévues pour l'essentiel dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « Informatique et libertés » en vigueur et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018.
Dans ce cadre, les utilisateurs devront informer le Délégué à la protection des données et se conformer à la procédure en vigueur pour la mise en œuvre d'un traitement de données à caractère personnel.
Conformément à la législation applicable à la protection des données personnelles, les principes directeurs à respecter dans le cadre de la mise en œuvre d'un traitement de données personnelles sont les suivants :

- le respect des finalités initiales du traitement ;

- la pertinence et l'exactitude des données au regard des finalités poursuivies ;
- l'information des personnes à la collecte des données et la conservation du recueil de leur consentement en cas de signature électronique ou manuscrite;
- le droit d'accès, de rectification ;
- le droit d'opposition ;
- la mise en œuvre de mesures de sécurité adaptée à la sensibilité des données
- traitées, résultant d'une étude d'impact pour les personnes privées en cas de
- divulgation, altération ou destruction des données les concernant.
- le contrôle rigoureux de la diffusion de données à caractère personnel l'attention de tiers extérieurs, en incluant notamment les clauses adaptées dans les contrats avec les sous-traitants.
- la destruction des données au-delà de la période de conservation prévue.[1]

[1] Référentiels CNIL : https://www.cnil.fr/fr/la-cnil-publie-trois-referentiels-pour-le-secteur-de-la-sante

8. SURVEILLANCE DU SYSTÈME D'INFORMATION

8.1. Contrôle

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.

8.2. Traçabilité

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 à minima :

- 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 personnel du service informatique respecte la confidentialité des données et des traces auxquelles il accède dans l'exercice de leur fonction, mais il peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

8.3. 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 au Responsable de la Sécurité du Système d'Information.

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

9. RESPONSABILITÉS ET SANCTIONS

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 ;
- Un licenciement et éventuellement des actions civiles ou pénales, selon la gravité du manquement.

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

I – OBJET et DOMAINE D'APPLICATION

Ce document a pour objet de préciser les objectifs de la charte de sécurité de l'information du Centre Hospitalier de Carcassonne. Ce document a pour vocation la sensibilisation, l'information des utilisateurs aux risques liés à la sécurité informatique et détermine les droits et devoirs de ces derniers.

Ce document s'applique à l'ensemble des agents de l'établissement et aux tiers (salariés suivis, prestataires externes, partenaires…) du Centre Hospitalier de Carcassonne qui peuvent avoir accès aux équipements informatiques et aux systèmes d'information et de communication du CH.

II - DEFINITION ET ABREVIATION

CHC : Centre Hospitalier de Carcassonne
RGPD : Règlement Général sur la Protection des Données
HN : Hôpital Numérique

III- REFERENCE

Programme Hôpital Numérique
Politique Générale de Sécurité des Systèmes d'Information de Santé
Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).Entrée en application le 25 mai 2018.

IV - DOCUMENTS ASSOCIES

DPI_PR_006 Gestion du dossier patient

V – MOTS-CLES

Sécurité
Système d'information
Hôpital numérique
RGPD
Informatique