



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 1 sur 11
version 01

Date d'application : 01/01/2020

Sommaire

1	OBJET ET DOMAINE D'APPLICATION	2
2	DESCRIPTION DE L'ACTIVITE.....	3
2.1	PROTECTION DE L'INFORMATION	3
2.2	USAGES DES RESSOURCES INFORMATIQUES	4
2.2.1	<i>Le poste de travail</i>	<i>4</i>
2.2.2	<i>Les logiciels et les applications.....</i>	<i>4</i>
2.2.3	<i>Les équipements mobiles de stockage</i>	<i>4</i>
2.3	USAGES DES OUTILS DE COMMUNICATION	5
2.3.1	<i>Surveillance du Système d'Information</i>	<i>5</i>
2.3.2	<i>Internet</i>	<i>5</i>
2.3.3	<i>Messagerie.....</i>	<i>6</i>
2.3.4	<i>Messagerie sécurisée de santé.....</i>	<i>7</i>
2.4	USAGE DES MOYENS D'ACCES	7
2.5	PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR	8
2.6	RESPONSABILITES - SANCTIONS	8
2.7	PROCESSUS DE DIFFUSION ET D'ACCEPTATION.....	9
3	DEFINITIONS ET ABREVIATIONS.....	9
4	TEXTES DE REFERENCE ET DOCUMENTS ASSOCIES	9
5	EVALUATION	10
6	DESTINATAIRES	11
7	CLASSEMENT – MOT-CLEF	11
8	GROUPE DE TRAVAIL.....	11
9	ANNEXES	11

Tableau des mises à jour

Version	Date	Page	Objet :
1	01/01/2020	Toutes	Création
	Rédaction	Vérification du contenu	Validation
NOM : Fonction :	Franck CHAMMING-RSSI Marie-Françoise GOURRIN -RSI Aurélien PARTONNAUD	Marine LE BRIS Directrice adjointe en charge des Opérations, de la Performance, des Finances, et du système d'information.	Elisabeth CALMON Directrice des Centres hospitaliers de Rambouillet et Ablis



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 2 sur 11
version 01

Date d'application : 01/01/2020

1 OBJET ET DOMAINE D'APPLICATION

La présente charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet du Centre Hospitalier de Rambouillet et de rappeler à leurs utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

Elle pose des règles permettant d'assurer la sécurité du système d'information de la structure, et la protection 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 la structure.

Cette charte a été validée par les instances dirigeantes du Centre Hospitalier de Rambouillet.

Elle constitue une annexe au Règlement Intérieur de la structure. Les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance.

La charte est mise à leur disposition sur le réseau informatique et affichée dans les locaux.

La présente charte concerne les ressources informatiques, les services internet et les services téléphoniques du Centre Hospitalier de Rambouillet, ainsi que tout moyen de communication permettant d'accéder à distance à ces ressources et services de la structure.

Il s'agit principalement des ressources suivantes :

- Ordinateurs de bureau ;
- Ordinateurs portables ;
- Tablette /Smartphones ;
- Scanners ;
- Imprimantes simples ou multifonctions ;
- Serveurs ;
- Autres petits matériels (lecteur codes à barres, systèmes de dictée numérique, ...etc.).

Cette charte s'applique à l'ensemble du personnel du Centre Hospitalier de Rambouillet, tous statuts confondus, et concerne notamment les utilisateurs permanents ou temporaires (stagiaires, internes, prestataires, fournisseurs, sous-traitants, ...) utilisant les moyens informatiques de la structure, que cet usage soit réalisé depuis les locaux de la structure ou à distance.



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 3 sur 11
version 01

Date d'application : 01/01/2020

2 DESCRIPTION DE L'ACTIVITE

2.1 Protection de l'information

La protection du patrimoine d'information du Centre Hospitalier de Rambouillet vise avant tout à assurer sa disponibilité, son intégrité, sa confidentialité et son auditabilité. Même si des dispositions organisationnelles et techniques sont prises au niveau de la structure, elles ne constituent qu'un premier niveau de protection. Chaque collaborateur a un rôle individuel essentiel à jouer.

Le personnel se doit de respecter le secret professionnel et/ou médical. Il doit faire preuve d'une discrétion absolue dans l'exercice de ses missions. 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.

Notamment, chaque utilisateur doit :

- Signaler à sa hiérarchie ou aux contacts désignés tout événement lui paraissant susceptible de compromettre la sécurité du système d'information ;
- Assurer la disponibilité et la pérennité des informations gérées au niveau de son environnement de travail en utilisant les différents moyens de sauvegarde et de duplication mis à sa disposition, si cette charge lui incombe ;
- Assurer la confidentialité des mots de passe ou codes utilisés pour les dispositifs de contrôle d'accès
- Assurer la protection des dispositifs qui participent au contrôle d'accès et qui lui sont confiés à titre strictement personnel (carte de la famille CPX, générateur de mot de passe unique, etc.).

Notamment, chaque utilisateur ne doit pas :

- Faire usage d'information dont il aurait connaissance sans qu'elles ne lui soient destinées, quand bien même celles-ci ne seraient pas explicitement protégées ;
- Transmettre sans autorisation des informations sensibles à l'extérieur de la structure, par le biais de la messagerie, d'outils en mode « cloud » ou de tout autre support (oral, papier...);
- Fournir des informations à une entité tierce (sous-traitant, personne extérieure à la structure) sans l'aval de la hiérarchie ;
- Transmettre des informations d'ordre professionnelles sur les réseaux sociaux ;
- Perturber volontairement le fonctionnement du système d'information par l'introduction de programmes malveillants ou par tout autre action (modification des configurations, détérioration du matériel,) ;
- Contourner les règles et restrictions d'utilisation des ressources mises à sa disposition par le Systèmes d'Information (SI).



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 4 sur 11
version 01

Date d'application : 01/01/2020

2.2 Usages des ressources informatiques

2.2.1 Le poste de travail

Dans le cadre de sa mission, un utilisateur peut se voir fournir un ou plusieurs postes de travail, fixe ou nomade. Il est de son devoir d'appliquer les règles de bonnes pratiques liées à ce type de matériel.

Notamment, chaque utilisateur doit :

Veiller à conserver en bon état de fonctionnement le matériel et les logiciels mis à sa disposition;

- Veiller à ce que les règles de verrouillage de session soient bien appliquées sur son matériel ;
- Signaler tout dysfonctionnement, anomalies, vol, perte ou sortie anormale du matériel au SI;
- S'engager à sécuriser son matériel avec les moyens mis à disposition par le SI (système antivol etc...) ;
- Utiliser les espaces de stockage des lecteurs réseau et l'intranet pour héberger ses données professionnelles.

Notamment, chaque utilisateur ne doit pas :

- Utiliser les équipements pour un usage personnel, sauf dans les limites fixées par le SI si ce dernier l'a autorisé explicitement ;
- Faire usage de postes de travail pour lesquels il n'a pas été explicitement autorisé ;
- Utiliser les équipements, les espaces de stockage des lecteurs réseau et l'intranet pour héberger ses données personnelles.

2.2.2 Les logiciels et les applications

L'utilisation de logiciels est soumise au respect du code de la propriété intellectuelle défini par le législateur.

Chaque utilisateur doit avoir conscience :

- Que l'utilisation de logiciels est soumise à l'acquisition de licences d'utilisation ;
- Que la loi protège les logiciels contre la copie ;
- Que sa responsabilité civile et pénale sera engagée en cas de copie ou de piratage de logiciel ;
- Qu'un logiciel sans licence, qu'il soit d'utilisation gratuite ou non, est une contrefaçon ou une source d'infection virale, voire d'intrusion par un tiers ;
- Qu'aucune installation de logiciel piraté sur le poste de travail, même pour utilisation à titre personnelle, ne sera admise.

2.2.3 Les équipements mobiles de stockage

L'usage de périphérique type clés USB ou disques externes doit rester exceptionnel, à noter :



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 5 sur 11
version 01

Date d'application : 01/01/2020

- Seuls les périphériques de stockage fournis par la structure sont autorisés ;
- Chaque périphérique de ce type doit faire l'objet d'un scan par l'antivirus à chaque utilisation par
- En règle générale, aucun objet communicant (smartphone, montre, bracelet, carte à puce...) ni aucun objet connecté de santé (dispositif médicaux, DMI ou objet en test) ne peut être connecté au réseau sans l'aval du SI, qui aura procédé à toutes les vérifications nécessaires à la validation du dispositif.

2.3 Usages des outils de communication

2.3.1 Surveillance du Système d'Information

Afin de répondre aux exigences légales et de permettre les investigations en cas d'incident de sécurité, le SI trace et peut faire analyser le trafic informatique entrant et sortant de son réseau. 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 personnel du SI respecte la confidentialité des données et des traces auxquelles ils sont amenés à accéder dans l'exercice de leur fonction. Ils peuvent être amenés à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs, dans le cadre de campagne de sensibilisation ou de phishing (campagne de faux emails en vue d'estimer la vulnérabilité des agents), dans le cadre du maintien en situation opérationnelle du SI, dans le cadre de contrôle de conformité de l'utilisation et des règles exposées dans la présente Charte.

2.3.2 Internet

Dans le cadre de sa mission, un accès à Internet peut être fourni à l'utilisateur.

Toute l'activité Internet de l'utilisateur peut donc être tracée. Ces traces ont cependant pour seule finalité la sécurité du système d'information et le respect des exigences légales. Leur accès est restreint aux seules personnes chargées de ces sujets. Elles ne sont en aucun cas disponibles aux autres personnels, ni pour quelque autre utilisation. Le SI se réserve le droit de bloquer certains contenus et sites web.



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 6 sur 11
version 01

Date d'application : 01/01/2020

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la consultation n'excède pas une durée raisonnable et présente une utilité au regard des fonctions exercées ou des missions à mener. L'utilisateur ne doit en particulier pas transférer de fichiers à usage personnel.

2.3.3 Messagerie

De même, l'utilisation de la messagerie est sujette à certaines bonnes pratiques.

Une vigilance accrue est nécessaire en ce qui concerne le traitement des pièces jointes.

Notamment, l'utilisateur doit :

- Rester prudent en ce qui concerne les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers envoyés habituellement par les contacts, et cela même si les pièces jointes sont analysées (Antivirus) avant d'être délivrées dans la messagerie ;
- Prévenir immédiatement le support informatique en cas de doute ou d'ouverture de pièces jointes piégées.

Notamment, chaque utilisateur ne doit pas :

- Répondre à une demande d'informations personnelles ou confidentielles (code confidentiel, mot de passe, etc...)
- Transférer automatiquement ou manuellement les mails professionnels vers des messageries privées externes à la structure. Seuls le cas de l'astreinte ou les cas de force majeure peuvent justifier ce type d'usage, à l'unique condition que ces modalités aient été préalablement prévues et validées par le service informatique ;
- Utiliser une adresse de messagerie professionnelle pour s'inscrire à des forums ou flux d'actualité qui ne sont pas liés aux métiers de la structure ;
- Inscrire une liste de diffusion professionnelle à des forums ou flux d'actualité quel qu'ils soient ;
- Utiliser la messagerie d'un collaborateur sans son consentement ;
- Relayer des messages type chaînes de lettre.
- Envoyer des informations nominatives confidentielles à l'extérieur de la structure en dehors des procédures sécurisées mises en place par le SI.

Un usage privé de la messagerie est toléré s'il reste exceptionnel. Il ne doit pas entraver la bonne marche du travail de l'utilisateur, ne pas être contraire aux intérêts du SI ni aux lois et règlements en vigueur, et doit rester raisonnable dans sa durée.

Les messages personnels doivent comporter explicitement la mention « privé » ou « personnel » au début de l'objet.

A défaut, les messages seront réputés relever de la correspondance professionnelle. Les messages marqués « privé » ou « personnel » ne doivent pas comporter de signature d'ordre professionnel à l'intérieur du message.



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 7 sur 11
version 01

Date d'application : 01/01/2020

En cas d'absence d'un agent et afin de ne pas interrompre le fonctionnement du service, le SI peut ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel.

En cas d'absence prolongée d'un agent (longue maladie), le responsable de service peut demander au SI, via une demande écrite au support (outil ticket ou mail), le transfert des messages reçus.

La messagerie est accessible à partir de l'adresse <https://courrier.ch-rambouillet.fr> sous réserve de saisir vos identifiants. Ce confort d'utilisation est mis à disposition en précisant toutefois que le rôle du Service Informatique consiste uniquement à maintenir l'accessibilité à cette fonctionnalité pendant ses jours d'ouverture. Par ailleurs, le Service Informatique n'assure pas d'assistance utilisateur.

2.3.4 Messagerie sécurisée de santé

La messagerie sécurisée à destination des professionnels de santé doit être utilisée en cas d'échanges de données médicales à caractère personnel entre professionnels de santé, que ce soit au sein de l'établissement ou vers l'extérieur.

Tout professionnel de santé est tenu de respecter le cadre juridique de l'échange des données de santé (article L1110-4 du code de la santé publique). Les données de santé à caractère personnel sont des données sensibles, protégées par la loi et dont le traitement est en outre soumis aux principes de la protection des données personnelles tels que définis par la loi Informatique et Libertés.

Le SI ne peut avoir accès aux données échangées, les informations étant chiffrées et inaccessibles pour tout non professionnel de santé.

Les dispositions mentionnées plus haut concernant les logiciels, la messagerie ainsi qu'internet s'appliquent également aux smartphones.

2.4 Usage des moyens d'accès

Chaque collaborateur dispose d'un (ou plusieurs) compte(s) nominatif(s) lui permettant d'accéder aux applications et aux SI de l'établissement. Ce compte est exclusivement personnel.

Pour utiliser ce compte nominatif, le collaborateur dispose d'un identifiant (« login ») et d'un mot de passe.

Chaque utilisateur est responsable de son compte et son mot de passe (ou du code personnel associé à la carte), et de la carte qui lui a été confiée le cas échéant, et de l'usage qui en est fait.

Il doit veiller à conserver secrets ses mots de passe et codes personnels, et à protéger sa carte CPS, CPE ou équivalent contre le vol, afin que personne ne puisse se connecter avec son propre compte.



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 8 sur 11
version 01

Date d'application : 01/01/2020

Notamment, chaque utilisateur doit :

- Fermer ou verrouiller sa session lorsqu'il quitte son poste ;
- Eteindre systématiquement son poste avant de quitter le soir pour les postes qui ne sont pas utilisés pendant la nuit ;
- Signaler toute tentative de violation de son compte personnel.

Notamment, chaque utilisateur ne doit pas :

- 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 ;
- Communiquer son mot de passe à qui que ce soit : ni à des collègues, ni à sa hiérarchie, ni au personnel du service informatique même pour une situation temporaire ;
- Mettre à la disposition de tiers non autorisés un accès aux systèmes et aux réseaux de l'établissement dont il a l'usage ;
- Contourner ou 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.

2.5 Procédure applicable lors du départ de l'utilisateur

Lors de son départ, l'utilisateur doit restituer au SI les matériels mis à sa disposition. Il doit préalablement effacer ses fichiers et données privées. Toute copie de documents professionnels doit être autorisée par le responsable de service de l'utilisateur.

Le compte et les données personnels à caractère professionnel (Mails, documents non partagés, ...) de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ (maximum 2 mois sur demande).

2.6 Responsabilités - Sanctions

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions à son encontre.

Des sanctions en interne peuvent être prononcées, elles consistent :

- Dans un premier temps, en un rappel à l'ordre émanant du SI, après avis du responsable de service de l'utilisateur en cas de non-respect des règles énoncées par la charte ;
- Dans un second temps, et en cas de renouvellement, après avis du responsable de service de l'utilisateur et de son supérieur hiérarchique, en des sanctions disciplinaires prises notamment après avis de la commission administrative paritaire compétente.



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 9 sur 11
version 01

Date d'application : 01/01/2020

Ces sanctions ne sont pas exclusives de l'application des dispositions du code pénal en matière de non-respect de l'utilisation des SI.

2.7 Processus de diffusion et d'acceptation

La présente charte est une annexe du règlement intérieur.

Elle est disponible sur l'intranet depuis l'ensemble des postes informatiques.

Toute mise à jour, donne lieu à une communication aux instances représentatives, mais également par courrier électronique et par courrier interne pour diffusion dans les services.

Toute réclamation, tout refus d'appliquer cette Charte en vigueur devra être formulé, de façon nominative, par courrier électronique ou courrier interne au secrétariat du SI.

3 DEFINITIONS ET ABREVIATIONS

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

- **Ressources informatiques** : les moyens informatiques, accessibles directement ou à distance ;
- **Outils de communication** : les moyens d'échanges ou de diffusion d'informations divers (téléphonie, web, messagerie, forum, etc.) ;
- **Utilisateurs** : les personnes autorisées à utiliser les ressources informatiques et les services internet de l'établissement.

4 TEXTES DE REFERENCE ET DOCUMENTS ASSOCIES

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 de santé à caractère personnel ;
- L'accès des patients et des professionnels de santé aux données médicales ;
- L'hébergement de données de santé ;
- 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 au regard du droit d'auteur.

La présente Charte tient compte de la réglementation en vigueur sur la sécurité de l'information et des droits et libertés reconnus aux utilisateurs.



Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 10 sur 11
version 01

Date d'application : 01/01/2020

Dispositions légales applicables concernant les responsabilités / sanctions:

- Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004. Dispositions Pénales :
 - o Code Pénal (partie législative) : art 226-16 à 226-24
 - o Code Pénal (partie réglementaire) : art R. 625-10 à R. 625-13
- Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. Dispositions pénales :
 - o Code pénal art 323
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).
- Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels.
Disposition pénale : Code Pénal : art L.335-2
- La loi n°92-685 du 22/07/1992 relative à la fraude informatique (article 323-1 à 323-7 du Code pénal) ;
- La loi du 10/07/91 relative au secret des correspondances émises par voie de télécommunication ;
- La loi n°92-597 du 01/07/1992 la législation relative à la propriété intellectuelle ;
- La loi du 04/08/1994 relative à l'emploi de la langue française ;
- La législation applicable en matière de cryptologie, notamment l'article 28 de la loi du 29/12/90 sur la réglementation des télécommunications dans sa rédaction issue de l'article 17 de la loi du 26/07/96 et par ses décrets d'application du 24/02/98, 23/03/98 et 17/03/99 ;
- La directive 96/9CE du 11 mars 1996 concernant la protection juridique des bases de données ;
- La loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé ;
- Loi n°227-23 du code pénal, qui criminalise le fait, de fixer, d'enregistrer ou de transmettre, en vue de sa diffusion, l'image ou la représentation d'un mineur qui présente un caractère pornographique.
- Loi n° 92-684 : du 22/07/1992 : sur la déclaration de tout fichier (de tout site) comportant des données nominatives,
- La loi relative aux infractions de presse du 29/07/1881, modifiée, sanctionnant notamment la diffamation, le négationnisme, le racisme et les injures et la loi relative aux infractions aux règles de cryptologie du 29/12/1990 modifiée le 26/07/1996

5 EVALUATION





Charte d'Accès et d'Usage du Système d'Information

PRO INF 010 Page 11 sur 11
version 01

Date d'application : 01/01/2020

6 DESTINATAIRES

L'ensemble du personnel de l'établissement.

7 CLASSEMENT – MOT-CLEF

Charte ; Sécurité ; Usage ; Systèmes d'information ; informatique

Cette charte est accessible dans le système de gestion documentaire de l'établissement (YES) et en accès plus rapide dans le classeur du processus « Système d'information »

8 GROUPE DE TRAVAIL

Liste des agents ayant participé à la rédaction de ce document :

Nom – Prénom	Fonction	Service
CHAMMING Franck	Responsable de la Sécurité du Système d'information	GCS SESAN
GOURRIN Marie-Françoise	Responsable du Système d'information	Système d'information du CH de Rambouillet
PARTONNAUD Aurélien	Stagiaire	Système d'information du CH de Rambouillet

9 Annexes