



# CHARTE UTILISATEUR DES SYSTÈMES D'INFORMATION 2017

Ce document est la propriété de Gustave Roussy. Les informations qu'il contient sont la propriété de l'établissement et ne peuvent pas être reproduites en totalité ou en partie ni être transmises par tout moyen sans l'autorisation écrite de l'Etablissement.

## CYCLE DE VIE DU DOCUMENT

### HISTORIQUE DU DOCUMENT

Version	Date	Description	Détails
1.0	2003	Charte Informatique - Politique de sécurité et règles d'usage	
2.0	10/2016	Charte Utilisateur des Systèmes d'Information (Refonte du document)	

### AUTEUR

Fonction	Nom	Date
Référent Sécurité des Systèmes d'Information / Architecte technique SI	LEMOINE Cédric	10/2016

### CONCERTATION / AVIS

Fonction	Nom	Date
Directoire	EGGUERMONT Alexander VARNIER Frédéric DUCREUX Michel MORICE Philippe FIZAZI Karim SOLARY Eric SCHLUMBERGER Martin CALVO Fabien MONTARON Anne BOURASSIN Philippe BENHAMOU Ellen DEUTCH Eric	04/2017
Comité de Direction	VARNIER Frédéric DUCREUX Michel MONTARON Anne BOURASSIN Philippe MEZAOUR Naima PUSTILCOV Ilia STEPANIAN Stéphane DAHER Valérie BIGOURDAN Philippe BRIERE Virginie MONS Muriel	02/2017

<b>Fonction</b>	<b>Nom</b>	<b>Date</b>
Direction de la recherche	SOLARY Eric BOUCARD David BOURSIN Yannick	03/2017
Direction de l'enseignement	SCHLUMBERGER Martin CROUAN Antoine GRELLIER Elodie	03/2017
Direction des Systèmes d'information	MEZAOUR Naima BUSET Marc MOUHEB Tahar GAVOILLE André DARLY Jimmy	01/2017
Direction des Ressources Humaines	BOURASSIN Philippe ALAYRAC Caroline	02/2017
Service des Affaires Juridiques	VEROTTE Nelly CHEVALLOT Sabine	02/2017
Comité d'Hygiène, de Sécurité et des Conditions de Travail		04/2017
Comité d'Entreprise		04/2017

## **VALIDATION**

<b>Fonction</b>	<b>Nom</b>	<b>Date</b>
Directeur Général	EGGERMONT Alexander VARNIER Frédéric	04/2017

## **LISTE DE DIFFUSION DU DOCUMENT**

<b>Fonction</b>	<b>Nom</b>	<b>Date</b>
Tout Utilisateur des Systèmes d'Information de Gustave Roussy		12/06/2017

## **SOMMAIRE**

Article 1 : Objet et Champ d'application .....	5
Article 2 : règles générales d'utilisation .....	6
Respect des lois, des réglementations et de la déontologie .....	6
Loi Informatique et Libertés .....	7
Article 3 : Accès aux Systèmes d'Information.....	7
Article 4 : Sécurité des équipements et des données .....	8
Gestion du poste de travail .....	8
Connexion des matériels informatiques aux réseaux d'entreprise.....	9
Gestion des données.....	10
Gestion des impressions .....	11
Gestion des anomalies .....	11
Article 5 : Usage de la messagerie électronique .....	12
Article 6 : Usage de l'Internet.....	12
Article 7 : Dispositions en cas d'absence ou départ d'un salarié .....	13
Article 8 : Traçabilité, procédure de contrôle et sanctions .....	13
Traçabilité et procédures de contrôle .....	13
Sanctions .....	14
Article 9 : Entrée en vigueur .....	14
ANNEXES .....	15
ANNEXE 1 : Cadre réglementaire et textes de référence .....	15
ANNEXE 2 : Bibliographie / Références documentaires .....	16
ANNEXE 3 : Sécurisation des mots de passe .....	17

## Article 1 : Objet et Champ d'application

Ce document constitue la Charte Utilisateur des Systèmes d'Information de Gustave Roussy.

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

- **Moyens informatiques** : Ce sont les moyens matériels (ordinateurs, serveurs, imprimantes, tablettes, smartphones) et logiciels mis à disposition dans le cadre des fonctions occupées et/ou missions, au sein de Gustave Roussy.
- **Systèmes d'Information** : Ensemble des éléments et règles participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein de l'Établissement, en provenance et vers ses partenaires externes.
- **Utilisateur** : toute personne, quel que soit son statut (stagiaires, internes, doctorants, chercheurs, prestataires, fournisseurs, sous-traitants, ...) ayant accès aux moyens informatiques professionnels dans le cadre de son emploi, d'une prestation ou d'un stage au sein de l'Établissement de Santé.
- **Données à caractère personnel** : Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement
- **Données de santé** : données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne
- **Politique Générale de Sécurité des Systèmes d'Information** : La politique de sécurité des Systèmes d'Information (PGSSI) de Gustave Roussy est un document fondateur, validé et appuyé par la direction générale. Elle précise les enjeux et les objectifs de sécurité du patrimoine informationnel de l'établissement.

Cette Charte s'applique à l'ensemble des Utilisateurs de Gustave Roussy utilisant les moyens informatiques de l'établissement sur site et/ou à distance.

L'objectif de la charte est de définir les bons usages, les droits et devoirs de chaque Utilisateur sur les Systèmes d'Information de Gustave Roussy, en regard de la Politique Générale de Sécurité des Systèmes d'Information (PGSSI) de l'établissement et des obligations législatives et réglementaires de la sécurité de l'information dans les établissements de santé.

Les aspects réglementaires font l'objet de **l'annexe 1**. Ils portent sur les grands thèmes suivants :

- Les droits et libertés reconnus aux utilisateurs des SI de Gustave Roussy, notamment la liberté d'expression et la liberté académique reconnue aux universitaires.
- Le traitement numérique des données, et plus précisément le traitement de données à caractère personnel relatives à la santé et au respect de la vie privée.
- 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 couvrant les données à caractère personnel relatives à la santé.
- 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.

## Article 2 : règles générales d'utilisation

Il est de la responsabilité de chaque utilisateur d'adopter un comportement professionnel lors de l'utilisation des Systèmes d'Information, en se conformant aux règles suivantes.

### Respect des lois, des réglementations et de la déontologie

Les utilisateurs se doivent d'être en conformité vis-à-vis des lois et des réglementations en vigueur, en particulier, le Code Pénal, le Code de la Santé Publique, le Code du Patrimoine, le Code des Postes et des Communications Électroniques portant notamment sur le secret de la correspondance, le Code de la Propriété Intellectuelle, la Loi Informatique et Libertés (LIL).

Il est notamment interdit pendant la durée du contrat de l'Utilisateur ainsi qu'après sa cessation :

- De diffuser à des tiers des informations relatives à Gustave Roussy, à ses salariés, à ses patients (violation du secret médical) ou à ses partenaires, sauf si la conduite des activités le nécessite.
- D'accéder aux données à caractère personnel relatives à la santé sans justification professionnelle.
- De diffuser des images et films pris au sein de Gustave Roussy des salariés et des patients sans leur autorisation explicite et celle de Gustave Roussy.
- De diffuser ou de télécharger des informations protégées par le droit d'auteur, qu'il s'agisse notamment d'écrits, d'images, de logiciels ou de bases de données, et de porter atteinte à tout signe distinctif appartenant à des tiers, en particulier aux droits de marques, notoires ou non, à toute dénomination sociale, enseigne, nom commercial et nom de domaine.
- De porter atteinte à la vie privée (sujets relatifs entre autres aux opinions politiques, philosophiques ou religieuses, aux origines ethniques, à la vie sexuelle ou à la santé des personnes).
- De publier tout propos contraire à la loi (notamment la diffamation, l'injure, les incitations aux crimes, à la discrimination, à la haine notamment raciale, le révisionnisme et l'apologie des crimes, la compromission de mineurs ou leur exposition à des messages à caractère violent ou pornographique, ou toute incitation à la consommation de substances interdites), aux règles éthiques et déontologiques.

- De publier tous contenus que la morale réprouve ou qui sont sans objet avec les activités professionnelles de l'Utilisateur.
- D'avoir toute action intentionnelle relevant de la fraude informatique (falsification, modification, suppression et introduction d'informations avec l'intention de nuire).
- De ne pas respecter les réglementations édictées en matière de traitement des informations à caractère personnel, dont la Loi Informatique et Libertés.

L'Utilisateur doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs lors de ses échanges électroniques par courriel, par publications sur des forums professionnels ou réseaux sociaux. Il n'émettra pas d'opinions étrangères à son activité professionnelle susceptibles de porter préjudice à l'Etablissement.

### **Loi Informatique et Libertés**

La constitution de fichiers informatiques comportant des données à caractère personnel, est encadrée par des règles strictes édictées par la Commission Nationale de l'Informatique et des Libertés (CNIL).

La création d'un traitement automatisé de données à caractère personnel suppose ainsi, préalablement à sa mise en œuvre, l'accomplissement d'une formalité auprès de la CNIL. Toute violation des principes et règles adoptés par la CNIL peut engager la responsabilité, y compris pénale, de Gustave Roussy et/ou de son auteur. De ce fait, toute personne ou service, souhaitant mettre en place un traitement de données à caractère personnel doit se rapprocher, au préalable, du correspondant Informatique et Libertés (CIL) », rattaché à la DSI de Gustave Roussy.

## **Article 3 : Accès aux Systèmes d'Information**

Chaque nouvel Utilisateur doit être préalablement déclaré et authentifié avant de bénéficier d'un accès au Système d'Information.

Les accès sont attribués selon les procédures d'habilitations tel que définies au sein de l'établissement en fonction des missions de l'utilisateur. Les habilitations liées aux données patients sont établies en lien avec le médecin DIM, la commission médicale et la direction des soins.

Tout départ ou changement d'affectation doit être signalé.

L'Utilisateur est responsable de son accès au Système d'Information.

Cet accès est strictement personnel et ne peut donc en aucun cas être prêté ou cédé. Il peut être retiré partiellement ou totalement, temporairement ou définitivement, en cas de non-respect de la Charte.

Les droits d'accès à tout ou partie des SI reposent sur la combinaison d'un identifiant et d'un authentifiant, tel que le mot de passe.

Une authentification forte assurant un niveau de sécurité plus élevé (mot de passe à usage unique, carte CPS) est mise en place pour certains usages.

**Les moyens d'authentification sont strictement personnels et confidentiels et ne doivent en aucun cas être communiqués à une tierce personne, y compris à son responsable hiérarchique ainsi qu'au support informatique.**

L'Utilisateur ne doit pas faire usage des moyens d'authentification ou des droits d'accès d'une tierce personne. De la même façon, il ne doit pas masquer sa propre identité.

L'Utilisateur s'engage à signaler au Référent Sécurité des Systèmes d'Information (RSSI) toute anomalie ou tentative de violation des accès au Système d'Information.

Les recommandations pour la sécurisation des mots de passe sont décrites en **annexe 3**.

## Article 4 : Sécurité des équipements et des données

L'utilisateur s'engage à respecter les règles décrites ci-dessous.

n°	règles	interdit	admis	recommandé	obligatoire	conditions / remarques
Gestion du poste de travail						
1	verrouillage de la session				X	L'Utilisateur doit verrouiller sa session dès qu'il quitte son poste de travail
2	détérioration des moyens informatique mis à disposition	X				
3	sécurisation des matériels (antivols, fermeture des locaux, armoires ...)				X	
4	déplacement des postes fixe (exemple: déménagement)	X				le déplacement des postes fixes doit être validé par la DSI
5	La configuration initiale du poste de travail doit être respectée				X	
6	Désactivation des outils de sécurité	X				
7	utilisation de droits étendus non justifié	X				L'Utilisateur aura des droits adaptés à sa fonction. Le principe du moindre privilège sera appliqué.



n°	règles	interdit	admis	recommandé	obligatoire	conditions / remarques
8	achats de logiciels ou matériels SI sans validation DSI	X				les achats doivent être validés par la DSI
9	Restitution du matériel appartenant à Gustave Roussy lors de la cessation ou de la suspension du contrat de l'utilisateur				X	
10	installation de logiciel ou périphérique par l'utilisateur	X				l'installation doit être validée et réalisée par les équipes de la DSI, ou bien par un personne habilitée
11	utilisation des moyens informatiques pour un usage personnel		X			Le poste de travail doit être utilisé pour les finalités professionnelles définies. Un usage personnel modéré est cependant toléré
12	utilisation du poste de travail par un tiers non autorisé/ habilité	X				L'Utilisateur n'autorisera pas l'accès aux moyens informatiques par un tiers non habilité. Il signalera toute anomalie au RSSI
<b>Connexion des matériels informatiques aux réseaux d'entreprise</b>						
13	connexion de matériel à usage professionnel sans validation/homologation de la DSI.	X				Tout équipement jugé non conforme par la DSI pourra, soit être déconnecté sans délai afin d'être remis en conformité, soit être isolé si la mise en conformité n'est pas possible
14	connexion d'un matériel réseau non validé par la DSI sur le réseau Gustave Roussy (switch, Hub, bornes WIFI, box ADSL, clé 3G/4G, modem smartphone...)	X				
15	installation de logiciel <b>personnel/privé</b> sur le SI ou connexion de matériel <b>personnel/privé</b> sur le réseau de Gustave Roussy	X				
16	connexion de clé USB ou disque dur amovible sur du matériel sensible de Gustave Roussy (nécessaire pour le soin patient)	X				
17	connexion de smartphones à la messagerie d'entreprise		X			En cas d'alerte sécurité, la DSI est susceptible de couper les accès à la messagerie sur l'équipement concerné.

n°	règles	interdit	admis	recommandé	obligatoire	conditions / remarques
18	connexion du matériel mobile (exemple PC portable) appartenant à Gustave Roussy, au réseau d'entreprise				X	le matériel devra être connecté à minima une fois par mois pour les mises à jour, notamment de l'antivirus.
<b>Gestion des données</b>						
19	stockage des données professionnelles nécessaires à la continuité de services sur des espaces réseaux fournis par la DSI				X	les espaces réseaux de stockage sont strictement réservés aux données professionnelles
20	stockage de données personnelles sur le disque dur local		X			l'espace doit être nommé sans ambiguïté "Privé". Les informations stockées doivent respecter les obligations légales (voir <b>Article 2</b> ) . Toutes données stockées en dehors des espaces nommés "privés" sont réputées professionnelles. Les données du disque dur local ne sont pas sauvegardées. La DSI se réserve le droit de demander la suppression de toutes données personnelles pouvant avoir un impact sur le bon fonctionnement des Systèmes d'Information
21	effacement ou altération des informations pouvant être nécessaires au bon déroulement des activités et/ou des services rendus par Gustave Roussy	X				voir <b>Article 8</b> pour manquement à cette règle
22	gestion des espaces de stockage: tri régulier et réévaluation des données conservées				X	L'Utilisateur doit veiller au bon usage de ses espaces de stockage
23	suppression des données privées, lors d'un départ définitif de Gustave Roussy				X	L'utilisateur devra procéder à la suppression des données privées (répertoire et messagerie) au plus tard le dernier jour effectivement travaillé au sein de Gustave Roussy
24	partage, sans autorisation, de données à caractère personnel dont celles de santé	X				le transfert de données à caractère personnel doit être cadré et sécurisé (juridiquement et techniquement). L'envoi de données de santé par mail est formellement interdit. Le Correspondant Informatique et Liberté (CIL) doit être sollicité dans le cas de besoin de transfert de données à caractère personnel

n°	règles	interdit	admis	recommandé	obligatoire	conditions / remarques
25	stockage des données Gustave Roussy à caractère personnel sur des espaces non fournis par Gustave Roussy (sauf convention)	X				risque de non-conformité des supports de stockage avec la réglementation en vigueur
26	stockage des données à caractère personnel, n'ayant pas de lien avec l'activité de Gustave Roussy, sur des espaces de stockage Gustave Roussy	X				L'utilisateur veillera à ne pas stocker les données provenant d'autres activités sur les espaces de stockage de Gustave Roussy
<b>Gestion des impressions</b>						
27	vigilance autour de l'impression des documents			X		L'utilisateur est responsable des données qu'il imprime. Il doit être attentif à l'imprimante sélectionnée et doit s'assurer de ne pas laisser l'accès aux documents sensibles par des personnes non habilitées
28	sécurisation des télécopieurs pour la réception ou l'envoi des données de santé				X	les télécopieurs doivent être situés dans des locaux adaptés, uniquement accessibles au personnel autorisé
<b>Gestion des anomalies</b>						
29	signalement de toute anomalie au support informatique				X	

## Article 5 : Usage de la messagerie électronique

L'Utilisateur est responsable du contenu et de la forme de tout message qu'il émet avec son adresse de messagerie Gustave Roussy

**Il est formellement interdit d'utiliser la messagerie électronique pour la communication de données de santé sous quelques formes que ce soit, sauf dans le cadre de l'utilisation de la messagerie sécurisée.**

L'Utilisateur :

- Doit veiller à ne pas porter atteinte à l'image ou à la réputation de Gustave Roussy. Il est interdit d'envoyer ou de faire suivre un message, contenant des informations illicites ou offensantes.
- Veille à ne pas divulguer son adresse électronique sur des forums ou sur des sites Internet non professionnels
- Doit faire preuve de la plus grande correction vis-à-vis de ses interlocuteurs, dans toutes les communications, qu'elles soient internes ou externes.
- S'astreint à faire régulièrement le tri et à évaluer la pertinence de conserver ou non les messages, particulièrement ceux contenant des pièces jointes. Tout contenu professionnel doit être stocké sur les espaces réseaux fournis par la DSI. **La messagerie électronique n'est pas un espace de stockage.**
- Veille à ne pas ouvrir des pièces jointes ou lien suspects notamment lorsque le correspondant est inconnu. Il s'engage à signaler ou demander conseil auprès du support informatique et du Référent Sécurité SI.
- S'interdit de faire une redirection automatique des messages vers une autre messagerie personnelle et/ou professionnelle. L'Utilisateur s'engage à utiliser la boîte aux lettres Gustave Roussy pour sa correspondance professionnelle.

Une utilisation privée occasionnelle et raisonnable est tolérée. Dans ce cas, un message privé doit être identifiable sans ambiguïté et enregistré dans un espace dédié.

## Article 6 : Usage de l'Internet

Seuls les sites Internet présentant un lien direct avec l'activité professionnelle ont vocation à être consultés.

Cependant, dans le cadre des nécessités de la vie courante, un usage personnel et raisonnable est admis, à condition qu'il soit conforme à la législation en vigueur et aux bonnes mœurs, et qu'il ne nuise pas aux tâches professionnelles incombant à l'Utilisateur. En outre, cet usage ne doit pas compromettre la disponibilité, la sécurité, la performance des Systèmes d'Information.

La réglementation impose une traçabilité nominative des accès Internet (loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme). L'Etablissement assure une traçabilité des navigations Internet et met en œuvre des outils de filtrage adaptés.

Gustave Roussy se réserve le droit de bloquer l'accès à tout site Internet non indispensable aux activités professionnelles, interférant avec le déroulement normal des activités ou présentant un risque d'incident de sécurité.

Le téléchargement de fichiers, de logiciels, de vidéos, d'images, de sons, ainsi que la visualisation en ligne de médias non liés à l'activité professionnelle sont interdits.

## **Article 7 : Dispositions en cas d'absence ou départ d'un salarié**

En cas de départ définitif :

- Le compte de l'Utilisateur sera désactivé
- Les traces relatives aux accès de l'Utilisateur seront conservées 12 mois.
- Les données professionnelles seront conservées dans le respect du secret professionnel.

En cas d'absence, les données réputées professionnelles restent accessible pour les besoins de services.

## **Article 8 : Traçabilité, procédure de contrôle et sanctions**

### **Traçabilité et procédures de contrôle**

Conformément à la réglementation, Gustave Roussy trace et contrôle les communications et l'usage de ses équipements pour, notamment :

- Etre à même de fournir des preuves nécessaires pour mener les enquêtes en cas d'incident de sécurité et de répondre à toute réquisition officielle présentée dans les formes légales notamment de la police judiciaire, conformément aux obligations légales de Gustave Roussy en la matière ;
- Contrôler le volume d'utilisation de la ressource, détecter des anomalies afin d'améliorer la qualité de service, faire évoluer les équipements en fonction des besoins ;
- Vérifier que les règles en matière de sécurité des Systèmes d'Information (fonctionnement de l'antivirus, installation des correctifs de sécurité...) sont correctement appliquées et conformes à la politique de sécurité ;
- Détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine.

Ce dispositif couvre les champs suivants :

- Accès internet,
- Usage de la messagerie électronique,
- Usage des téléphones et télécopieurs,
- Accès à l'ensemble des ressources des SI.

Ces données sont archivées pendant une durée maximale d'un an.

### **Sanctions**

La violation de la présente charte constituant une faute professionnelle susceptible d'entraîner la mise en œuvre d'une sanction disciplinaire, Gustave Roussy se réserve le droit d'engager une procédure disciplinaire à l'encontre de l'Utilisateur.

La procédure disciplinaire peut induire une suspension provisoire ou définitive des accès au SI pour l'Utilisateur concerné.

En cas de suspension ou interruption des droits d'accès de l'Utilisateur au SI, Gustave Roussy permettra à l'Utilisateur la récupération des données personnelles.

Concernant les Utilisateurs liés par un contrat de mission, de prestation de service, ou une convention, tels que les intérimaires, les stagiaires, les partenaires ou les fournisseurs, en cas de violation des règles de bon usage des SI, Gustave Roussy se réserve la possibilité d'une rupture dudit contrat ou de ladite convention, ainsi que la possibilité de poursuites judiciaires à l'égard de l'entreprise d'origine et/ou de la personne concernée.

### **Article 9 : Entrée en vigueur**

Conformément à l'article L. 6162-7 du Code de la santé publique, la Direction Générale de Gustave Roussy a arrêté la présente charte après avis et concertation (se référer à la partie « cycle de vie du document » en page 2 et 3).

Cette Charte est annexée au Règlement intérieur, et diffusée sur l'intranet.

La Charte Utilisateur des Systèmes d'Information entre en vigueur à compter de la date de publication mentionnée dans la partie « liste de diffusion du document » en page 3.

Elle sera modifiée en fonction du contexte législatif et réglementaire et des évolutions des nouvelles technologies.

## ANNEXES

### ANNEXE 1 : Cadre réglementaire et textes de référence

La présente Charte Utilisateurs du SI respecte la réglementation sur la sécurité de l'information en vigueur et les droits et libertés reconnues aux Utilisateurs. La réglementation porte sur les grands thèmes suivants :

- **La protection de la sécurité des systèmes d'informations et des données :**
  - Protection des logiciels et des bases de données ;
  - Lutte contre la cybercriminalité ;
  - Intrusion ou maintien frauduleux ;
  - Altération et entrave au fonctionnement ;
  - Droit d'auteur ;
  - Signature électronique.
- **La protection des droits des données personnelles :**
  - Secret professionnel ;
  - Secret médical et droit d'accès des professionnels de santé et patients aux données de santé ;
  - Secret des correspondances ;
  - Respect de la vie privée.

#### Principaux textes correspondants :

- **Code civil**

Article 9 (droit au respect de la vie privée);  
Article 1367 (fiabilité de la signature électronique).

- **Code pénal**

*Atteinte au secret professionnel*

Article 226-13 (révélation d'une information à caractère secret du fait de sa profession);

Article 226-14 (autorisation légale à la révélation du secret).

*Atteinte au secret des correspondances :*

Articles 226-15 (violation du secret de correspondance);

Article 432-9 (atteinte par une personne chargée d'une mission de service publique).

*Atteintes aux systèmes de traitement automatisé de données :*

Article 323-1 (intrusion illicite);

Article 323-2 (entrave au fonctionnement du système d'information);

Article 323-3 (introduction illicite de données);

Article 323-3-1 (mise à disposition d'équipement pour la commission d'infractions).

- **Code de la santé publique**

Article L1110-4 (secret médical et partage d'informations);

Article **L1111-7** (accès au dossier médical);  
Article **L1111-8** (hébergement de données de santé).

▪ **Code de la propriété intellectuelle**

Articles **L335-3 et suivants** (protection droit d'auteur, lutte contre la contrefaçon);  
Articles **L342-1 et suivants** (droits des protecteurs de base de données);  
Articles **L343-1** (atteintes aux droits des protecteurs de base de données).

- Loi **n°78-17 du 6 janvier 1978** dite « informatique et libertés » modifiée par la loi n°2004-801 du 6 août 2004;
- Directive européenne 96/6 CE du 11 mars 1996 concernant la protection juridique des bases de données transposé dans le code de la propriété intellectuelle par la loi **n°98-536 du 1<sup>er</sup> juillet 1998**;
- Loi **n°2002-303 du 4 mars 2002** relative aux droits des malades et à la qualité du système de santé;
- Loi n°88-19 du 5 janvier 1988, complétée par la loi **n°2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique;
- Loi **n°2006-64 du 23 janvier 2006** relative à la lutte contre le terrorisme;
- Décret **n°2006-669 du 24 mars 2006** relatif à la conservation des données des communications électroniques;
- Loi **n°2009-669 du 12 juin 2009** favorisant la diffusion et la protection de la création sur internet;
- Loi **n°2009-1311 du 28 octobre 2009** relative à la protection pénale de la propriété littéraire et artistique sur internet dite « loi Hadopi 2 »;
- Décret **n°2006-6 du 4 janvier 2006** relatif à l'hébergement de données de santé à caractère personnel;
- Décret **n°2007-960 du 15 mai 2007** relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique.

**ANNEXE 2 : Bibliographie / Références documentaires**

- PGSSI v3.0 2017 - Gustave Roussy
- Guide professionnel de la santé – CNIL
- Guide d'hygiène informatique - ANSSI
- Vigipirate Objectifs de cyber sécurité (2014) - ANSSI
- RGS v2.0 (Référentiel Général de Sécurité) – ANSSI
- Fiche pratique 7 : charte type d'accès et d'usage du Système d'Information – ASIP
- Charte de l'Utilisateur – INSERM
- Charte informatique – CNRS
- Charte de déontologie - RENATER



### ANNEXE 3 : Sécurisation des mots de passe

Les règles suivantes sont à appliquer pour la sécurisation des mots de passe :

- Ne pas conserver les mots de passe sur des supports non sécurisés, notamment sur papier facilement accessible (cahier, post-it, tableau, manuels, document d'exploitation ...)
- Ne pas stocker les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet).
- Eviter d'utiliser la fonction « se souvenir » sur les navigateurs internet.
- Ne pas utiliser le mot de passe pour l'ensemble des accès et bien distinguer les mots de passe professionnels et personnels.
- Ne pas utiliser la messagerie personnelle pour véhiculer les mots de passe professionnels.
- Ne jamais demander à un tiers de créer un mot de passe pour vous.
- Renouveler vos mots de passe avec une fréquence raisonnable (Tous les 90 jours).
- Composer votre mot de passe avec 8 caractères minimum, contenant des chiffres et des caractères spéciaux. Il est recommandé d'utiliser une « phrase clé » pour mémoriser son mot de passe (exemple : « **Je travaille à Villejuif depuis 5 ans.** » → Mot de passe = JetràVide5an.).

114, rue Édouard-Vaillant  
94805 Villejuif Cedex - France

[www.gustaveroussy.fr](http://www.gustaveroussy.fr)