

LES GUIDES DE L'AP-HP

# Charte du bon usage du système d'information de l'AP-HP

DE L'ASSISTANCE PUBLIQUE-  
HÔPITAUX DE PARIS

EDITION 2023

# Charte du bon usage du système d'information de l'AP-HP

## Synthèse des principales règles

- Il est de la responsabilité de chaque utilisateur d'adopter un comportement professionnel.
- La configuration initiale du poste de travail doit être respectée.
- La connexion au SI d'équipements non fournis par l'AP-HP est soumise à des règles strictes.
- Les ordinateurs doivent être protégés physiquement.
- Les sessions des ordinateurs doivent être verrouillées en cas d'absence.
- Les informations professionnelles nécessaires à la continuité des activités doivent être sauvegardées sur les répertoires réseaux mis à disposition.
- Les supports amovibles doivent être utilisés avec vigilance.
- Les documents sensibles doivent être rapidement récupérés aux imprimantes.
- Les moyens de télécommunication sont à usage professionnel avant tout.
- Les téléphones portables et smartphones doivent être protégés par un code.
- Les mots de passe doivent respecter les règles de bonnes pratiques de la CNIL.
- L'accès aux informations se fait au regard des nécessités professionnelles pour l'exercice de l'activité de chaque utilisateur.
- Internet et la messagerie électronique sont à usage professionnel avant tout.
- L'accès à Internet avec les équipements de l'AP-HP doit se faire au travers des infrastructures fournies par l'AP-HP.
- L'accès à des sites Internet initialement bloqués par l'AP-HP, est interdit sauf cas dérogatoire.
- La publication depuis le Système d'Information de l'AP-HP doit se faire dans le respect de la loi et des codes de déontologie professionnelle.
- Les outils de communication audiovisuelle par Internet doivent être utilisés avec vigilance pour l'échange d'informations confidentielles

## **Préambule et objet**

La prise en charge des patients et l'activité de l'AP-HP dépendent de la continuité du fonctionnement du système d'information (SI) de l'AP-HP. L'AP-HP est soumise aux obligations législatives et réglementaires propres aux informations numérisées et en particulier pour les données à caractère personnel relatives à la santé.

La sécurité et le bon fonctionnement du Système d'Information sont l'affaire de tous et découlent d'une action à la fois collective et individuelle. Chacun doit être conscient de ses droits, mais aussi de ses devoirs tant vis-à-vis des patients pris en charge que de l'AP-HP. La Charte d'utilisation du système d'information de l'AP-HP, ou Charte informatique, s'inscrit dans le cadre de la Politique Générale de Sécurité du Système d'Information (PGSSI) de l'AP-HP, validée par la Direction Générale. Elle est de ce fait, un document de référence pour l'ensemble des entités de l'AP-HP et constitue une annexe au règlement intérieur. Les professionnels de santé, les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance et l'appliquer. La Charte est mise à leur disposition sur l'Intranet et affichée dans les locaux de l'AP-HP.

## **Art.1 Champ d'application de la charte informatique**

### **1.1 Les utilisateurs du système d'information de l'AP-HP**

La Charte informatique s'applique à l'ensemble des utilisateurs du Système d'Information de l'AP-HP. Est considérée comme « Utilisateur du SI », toute personne amenée à utiliser les ressources du SI quel que soit son statut (par exemple le professionnel de santé ou médico-social, l'agent de l'AP-HP, le personnel intérimaire, la personne en formation, le stagiaire, le prestataire ou le partenaire), son niveau hiérarchique et son lieu d'accès.

Les règles de la Charte informatique doivent, par conséquent, être prises en compte par le personnel des entités sous-traitantes et des partenaires externes accédant au SI de l'AP-HP. Les entités chargées des relations contractuelles et opérationnelles avec ses sous-traitants

ou partenaires, doivent donc s'assurer du respect des règles de bon usage sur le périmètre d'actions impactant le SI de l'AP-HP. En particulier, la Trésorerie Générale doit s'assurer du respect des règles de bon usage du système d'information sur le périmètre du SI commun avec l'AP-HP. Une décision du Directeur général sera prise, après concertation avec les instances représentatives du personnel, sur les conditions générales d'utilisation par les organisations syndicales du système d'information de l'AP-HP.

## 1.2 Système d'information et de communication

Le système d'information et de communication de l'AP-HP est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques (USB et autres), équipements biomédicaux ou de gestion technique centralisée connectés au réseau, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs et imprimantes multifonctions, téléphones, logiciels et progiciels, fichiers, données et bases de données, système de messagerie, Intranet, Extranet, abonnement à des services interactifs ainsi que toutes les procédures, consignes d'utilisation et modes opératoires.

Les règles édictées dans ce document, s'appliquent également à l'ensemble des équipements informatiques non fournis par l'AP-HP et interagissant avec les ressources internes du SI de l'AP-HP. Il s'agit, à titre d'illustration des équipements personnels, ou fournis par des partenaires, et autorisés à être connectés au SI de l'AP-HP, comme décrit dans la suite du document.

## 1.3 Cadre législatif et réglementaire

Le cadre législatif et réglementaire de la sécurité de l'information dans les établissements de santé est large. Il fait l'objet de l'annexe 1. Il porte sur les grands thèmes suivants :

- Les droits et libertés reconnus aux utilisateurs du SI de l'AP-HP, notamment la liberté d'expression, les libertés syndicales, 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 le 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.

La présente Charte informatique tient compte de la réglementation sur la sécurité de l'information en vigueur.

#### Art.2 Les règles générales d'utilisation

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

### **2.1 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 :

- De diffuser des informations relatives à l'AP-HP, à ses agents, 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 l'AP-HP des agents et des patients sans leur autorisation explicite et celle de l'AP-HP.
- 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 d'éthique et de déontologie.

- Tout acte relevant de la fraude informatique (falsification, modification, suppression et introduction d'informations avec l'intention de nuire).
- Tout non-respect des réglementations édictées en matière de traitement des informations à caractère personnel, dont la Loi Informatique et Libertés.

## 2.2 Loi informatique et libertés

La constitution de fichiers informatiques comportant des données à caractère personnel, c'est-à-dire permettant d'identifier directement ou indirectement une personne physique, 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 du correspondant informatique et libertés de l'AP-HP pour les traitements relevant de son champ de compétence ou de la CNIL le cas échéant. Toute violation des principes et règles adoptés par la CNIL peut engager la responsabilité, y compris pénale, de l'AP-HP 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 référent Loi Informatique et Libertés (LIL) de son GH/Site/PIC, généralement rattaché à la DSI des Groupes Hospitaliers.

## Art.3 Sécurité des équipements mis à disposition

### 3.1 Sécurité du poste de travail

**La configuration initiale du poste de travail doit être respectée.**

La configuration du matériel de l'AP-HP a été étudiée afin de garantir le bon fonctionnement et la sécurité du Système d'Information. De ce fait :

- Elle ne doit jamais être modifiée et doit être conservée telle qu'elle a été définie par la Direction des Systèmes d'Information de l'AP-HP.
- De même, afin de limiter tout risque de propagation de virus à travers le réseau informatique, l'utilisateur ne doit jamais désactiver les outils de sécurité, tel que l'antivirus, ou modifier leur paramétrage.
- Afin de limiter les risques d'intrusion, les postes de travail informatiques, quand ils sont connectés au réseau de l'AP-HP, ne doivent pas être connectés simultanément à

un autre réseau.

Dans le cadre du respect de la propriété intellectuelle et des règles d'usage des licences, la copie des logiciels mis à sa disposition par l'AP-HP est interdite, hormis les copies de sauvegarde. Chaque utilisateur doit se conformer aux restrictions d'utilisation des logiciels fournis par l'AP-HP.

### **Les ordinateurs doivent être protégés physiquement.**

Chacun doit veiller à utiliser les moyens de protection fournis par l'AP-HP tels que les câbles antivol et les armoires à clé, afin d'éviter les vols ou la dégradation des équipements. Par ailleurs, les postes de travail fixes ne doivent pas être déménagés d'un local à un autre sans autorisation.

### **Les sessions des ordinateurs doivent être verrouillées en cas d'absence.**

Afin d'empêcher tout risque d'intrusion dans le Système d'Information pouvant mener à des incidents de sécurité, telle que la fuite d'informations, chaque utilisateur doit s'assurer d'avoir verrouillé sa session, s'il est amené à laisser sa station de travail sans surveillance ou à quitter son bureau

### **Les informations professionnelles nécessaires à la continuité des activités doivent être sauvegardées sur les répertoires réseaux mis à disposition.**

• L'AP-HP met à la disposition des utilisateurs des espaces de stockage afin qu'ils puissent sauvegarder et partager des informations. Les utilisateurs doivent être vigilants quant à l'usage qu'ils font de ces répertoires partagés, et sont responsables des informations qu'ils stockent sur ces ressources. Les documents électroniques et les messages professionnels qui reflètent les activités de l'AP-HP, ou qui formalisent les différentes étapes d'une tâche, d'une décision, d'une procédure, dans le cadre des missions liées à l'activité de l'AP-HP, sont à archiver.

- Les utilisateurs ne doivent jamais effacer, supprimer ou modifier des informations pouvant être nécessaires au bon déroulement des activités et des services rendus par l'AP-HP.
- Ils doivent procéder à des sauvegardes régulières des informations professionnelles, stockées localement sur leur ordinateur, sur les répertoires réseaux et ce, afin d'éviter tout risque de perte d'informations (en cas de défaillance de l'ordinateur par exemple).
- Pour les informations sensibles, l'utilisateur veillera à les stocker dans des répertoires avec des droits réservés aux seules personnes légitimes à y accéder (tels que les répertoires partagés entre les membres d'un service par exemple). En cas de doute, il pourra se renseigner auprès du support SI.

- Les informations sauvegardées sur les répertoires, y compris les répertoires personnels, doivent être conformes aux lois et règlements en vigueur (interdiction, entre autres, de stocker des informations à caractère pédopornographique, raciste, diffamatoires ou des copies illégales de logiciels, de films, de musique ou d'images).
- Toute personne, ou service, souhaitant un conseil sur le formalisme et les modalités d'archivage, numérique ou papier, doit se rapprocher du Service des Archives de l'AP-HP. .

## 3.2 Sécurité des autres moyens du SI

### **Les supports amovibles doivent être utilisés avec vigilance.**

Les supports amovibles, tels que les clés USB, les appareils photos, les lecteurs MP3, ou les disques externes, sont susceptibles d'héberger des programmes informatiques pouvant porter atteinte à l'intégrité du Système d'Information (par exemple des virus, des vers, ou des chevaux de Troie) et par conséquent, menacer sa sécurité, et ce, parfois à l'insu de l'utilisateur. Leur installation est fortement déconseillée.

Chaque personne doit porter une attention particulière à la protection des supports amovibles contenant des informations couvertes par le secret professionnel.

Ainsi, il est demandé à chaque personne de privilégier l'usage de matériels fournis par l'AP-HP, et de ne les connecter qu'à des postes de travail sécurisés (pourvus d'un antivirus). De plus, chaque utilisateur doit veiller à ne pas connecter des supports amovibles dont l'origine lui paraît suspecte.

Les supports amovibles utilisés, au regard la sensibilité des données stockées, assurent automatiquement la protection de leur contenu par chiffrement. Dans le cas contraire, l'utilisateur est chargé de chiffrer et déchiffrer les informations en utilisant les logiciels mis à disposition par l'AP-HP.

En cas de doute sur la fiabilité d'un support amovible, l'utilisateur doit se rapprocher du support SI de son Groupe Hospitalier ou de son site, qui pourra lui indiquer comment procéder à son analyse.

### **Les documents sensibles doivent être rapidement récupérés aux imprimantes.**

Les imprimantes sont souvent partagées, de ce fait, tout document confidentiel (contenant des données à caractère personnel relatives aux patients ou aux agents, ou des informations financières par exemple) doit être récupéré rapidement.



**Les moyens de télécommunication sont à usage professionnel avant tout.**

L'AP-HP met à la disposition des utilisateurs des moyens de télécommunication tels que les télécopieurs (fax) ou les téléphones. Ces moyens de télécommunication sont réservés à des fins strictement professionnelles. Cependant, dans le cadre des nécessités de la vie courante, un usage personnel est toléré 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 ou à la bonne conduite des activités de l'AP-HP. .

En outre, cet usage ne doit pas compromettre la sécurité du Système d'Information et la disponibilité des services de télécommunication mis à la disposition des utilisateurs.

**Les téléphones portables et smartphones doivent être protégés par un code.**

Les téléphones portables et les smartphones, permettant de stocker et/ou d'accéder aux informations parfois confidentielles de l'AP-HP, doivent être protégés. Lorsque cela est techniquement possible, l'utilisateur doit définir un code PIN et un code de déverrouillage en prenant soin de choisir un code suffisamment complexe (en évitant les codes du type « 0000 » ou « 1234 »).

**Accès à distance et utilisation en situation de mobilité**

L'accès à distance offre la possibilité d'utiliser le système d'information de l'AP-HP de manière équivalente à celle qui serait réalisée depuis les locaux de l'AP-HP. Il est notamment adapté au télétravail, aux astreintes, à répondre aux crises et aux difficultés d'accès à son lieu de travail.

L'utilisateur s'engage à utiliser exclusivement le dispositif d'accès à distance mis à disposition par l'AP-HP et à en respecter les règles d'utilisation. Il veillera notamment à ce qu'aucune autre personne ne voit ou n'accède aux données de l'AP-HP. Il veillera au respect de la confidentialité des données.

## **Art.4 Droit d'accès et mots de passe**

Les droits d'accès à tout ou partie du SI de l'AP-HP reposent sur l'usage d'un compte d'accès strictement personnel composé d'un identifiant (par exemple le code APH ou le code prestataire) et d'un authentifiant, tel que le mot de passe ou des cartes de professionnels de santé (CPS) ou de personnels d'établissement (CPE) avec son code confidentiel.

Les moyens d'authentification sont strictement personnels et confidentiels et ne doivent en aucun cas être communiqués à une tierce personne. En cas d'intervention du support SI nécessitant la communication de l'authentifiant, celui-ci devra être changé

Les utilisateurs sont seuls responsables des actions réalisées depuis leurs comptes d'accès à leurs ordinateurs.

L'encadrement s'assure que les droits d'accès accordés aux utilisateurs sous sa responsabilité correspondent à leurs missions.

Les droits d'accès associés à ces comptes feront l'objet de revues régulières afin de corriger toutes anomalies (droits non adéquats au regard des activités des utilisateurs par exemple). De plus, en cas de mobilité d'un utilisateur du SI, ses droits d'accès seront modifiés ou désactivés (annexe 2).

En cas de départ définitif :

- Le compte de l'utilisateur sera désactivé.
- Les traces relatives aux accès de l'utilisateur seront conservées 12 mois.
- Il appartient à l'utilisateur de récupérer ou d'effacer les données identifiées comme « privées » ou « personnelles », dans le respect de la charte informatique, avant son départ. Elles seront systématiquement effacées après le départ de l'agent et après information de celui-ci.
- Les données professionnelles seront conservées dans le respect du secret professionnel.

L'encadrement s'assure que les droits d'accès accordés aux utilisateurs sous sa responsabilité quittant leur service sont bien révoqués ou désactivés.

L'utilisation de comptes non personnels (par exemple les comptes génériques ou les comptes partagés) doit rester exceptionnelle. Dans le cas où l'utilisateur y a accès, il est responsable de l'usage qu'il fait de ces derniers, et se doit de respecter les règles de sécurité du présent document, au même titre que pour son compte personnel.

**Les mots de passe doivent respecter les règles de bonnes pratiques de la CNIL.**

L'utilisateur doit définir un mot de passe complexe, difficile à deviner par un tiers et doit veiller à le modifier régulièrement afin d'éviter toute usurpation de son identité. Vous trouverez toutes les informations et conseils sur le site intranet dédié à la sécurité de l'information à l'adresse <http://ssi.aphp.fr>.

**L'accès aux informations se fait au regard des nécessités professionnelles pour l'exercice de l'activité de chaque utilisateur.**

Tous les personnels de l'AP-HP sont soumis au secret professionnel dont le secret médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données à caractère personnel relatives à la 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. Afin de garantir la qualité des services rendus par l'AP-HP et l'intégrité de son SI, chaque utilisateur ne doit accéder qu'aux seules informations nécessaires à la réalisation de son activité professionnelle et dans le respect des principes de confidentialité. Les informations consultées dans le cadre de tâches professionnelles ne doivent être utilisées qu'à ce titre.

Lorsqu'une personne estime qu'elle ne dispose pas des habilitations adaptées au bon exercice de ses activités professionnelles, elle doit s'adresser à son Responsable hiérarchique afin de les faire modifier.

## **Art.5 Utilisation d'Internet**

Internet rend accessible à tous un très grand nombre d'informations, au travers de sites offrant un degré de confiance très variable. De plus, l'intégrité et la confidentialité des informations qui y sont transmises ne peuvent être garanties. De ce fait, les utilisateurs doivent être conscients que les informations transitant sur Internet peuvent, à tout moment, être interceptées par des tiers.

### **Internet est à usage professionnel avant tout.**

L'AP-HP met à la disposition des utilisateurs l'accès à Internet. Cet accès est réservé à des fins strictement professionnelles. Cependant, dans le cadre des nécessités de la vie courante, un usage personnel (réservation de billets de trains, consultation de plans ou horaires, appels d'urgence...) est toléré, 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 ou à la bonne conduite des activités de l'AP-HP.

En outre, cet usage ne doit pas compromettre la sécurité du Système d'Information et la disponibilité des services Internet, mis à la disposition des utilisateurs.

La consultation de sites Internet ou le téléchargement de fichiers qui pourraient, au sens le plus large, être considérés comme illégaux ou immoraux sont interdits, sauf si cela est expressément requis dans le cadre des activités professionnelles des utilisateurs.

**L'accès à Internet avec les équipements de l'AP-HP doit se faire au travers des infrastructures fournies par l'AP-HP.**

Depuis les locaux de l'AP-HP, l'accès à Internet avec les équipements de l'AP-HP est autorisé à travers les infrastructures configurées et fournies par l'AP-HP. Il est par conséquent, strictement interdit, d'utiliser des réseaux WIFI externes dans les locaux de l'AP-HP pour accéder à Internet. De même, il est interdit d'installer et d'utiliser une borne WIFI privée au sein de l'AP-HP sans autorisation expresse du représentant habilité de l'AP-HP

Dans le cas des utilisateurs nomades, se trouvant à l'extérieur des locaux de l'AP-HP, l'accès au réseau de l'AP-HP au travers d'accès Internet externes (par exemple Internet personnel ou bornes WIFI) est autorisé, sous réserve qu'ils veillent à utiliser les moyens de connectivité sécurisés fournis par l'AP-HP (par exemple l'accès VPN). Cet accès se fait sur demande à la DSI sous couvert de l'autorité hiérarchique.

**L'accès à des sites, initialement bloqués par l'AP-HP, est interdit sauf cas dérogatoire.**

L'AP-HP se réserve le droit de bloquer l'accès à tout site Internet non indispensable aux activités professionnelles, interférant avec le déroulement normal des activités de l'AP-HP (exemple : problèmes de débit Internet et de saturation réseau) ou présentant un risque d'incident de sécurité. Par ailleurs, les sites contenant des éléments pornographiques, indécents, incitants à la haine, insultants ou relatifs au piratage informatique sont bloqués par les règles de filtrage.

**Gestion des communications chiffrées.**

L'AP-HP se réserve le droit de déchiffrer les flux de communication chiffrés à destination de l'Internet.

Cette fonction est utilisée pour identifier les logiciels malveillants, protéger le patrimoine informationnel ou encore de détecter des flux sortants anormaux. Les sites relevant des catégories « Santé » et « Services financiers » sont exclus de cette analyse.

**La publication depuis le Système d'Information de l'AP-HP doit se faire dans le respect de la loi et des codes de déontologie professionnelle.**

La publication de contenu professionnel et/ou personnel, depuis le Système d'Information de l'AP-HP, sur des blogs, forums, réseaux sociaux, ou sites non professionnels, c'est-à-dire non partenaires ou non administrés par l'AP-HP, engage la responsabilité de l'utilisateur

et l'image de l'AP-HP. Cette publication doit donc se faire dans le respect de principes énumérés à l'article 2 et des codes de déontologie professionnelle pour les professions qui en disposent

**Les outils de communication audiovisuelle par Internet doivent être utilisés pour l'échange d'informations confidentielles avec vigilance.**

Les outils de communication audiovisuelle par Internet (téléphonie, visio-conférence) peuvent comporter des failles pouvant constituer une menace pour la sécurité du Système d'Information et des informations échangées (possibilité d'interception des échanges par une tierce personne ou contournement des moyens de protection tels que les pare-feu par exemple).

## **Art.6 Utilisation de la messagerie électronique**

**La messagerie électronique est à usage professionnel avant tout.**

L'AP-HP met à la disposition des utilisateurs une messagerie électronique. Cette messagerie est réservée à des fins strictement professionnelles. Cependant, dans le cadre des nécessités de la vie courante, un usage personnel est toléré 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 et à la bonne conduite des activités de l'AP-HP. En outre, cet usage ne doit pas compromettre la sécurité du Système d'Information et la disponibilité des services de messagerie, mis à la disposition des utilisateurs.

L'utilisateur est responsable du contenu et de la forme de tout message qu'il émet avec son adresse de messagerie AP-HP. Il ne doit pas se faire passer pour une autre personne en utilisant son adresse et ne doit pas modifier les documents reçus.

Tout message envoyé depuis l'adresse professionnelle AP-HP, associe nécessairement l'AP-HP à son contenu. L'utilisateur doit donc veiller à ce que celui-ci ne porte pas atteinte à l'image ou à la réputation de l'AP-HP. De ce fait, il est interdit d'envoyer ou de faire suivre un message, contenant des informations illicites ou offensantes.

L'utilisation d'une messagerie sécurisée est obligatoire pour tout échange de données à caractère personnel relatives à la santé. Pour les échanges de données personnelles de santé avec le patient, le professionnel de santé doit obtenir son accord éclairé.

## **Art.7 Remontées des incidents par les utilisateurs**

Traçabilité et procédures de contrôle anomalie suspectée ou avérée concernant le SI de l'AP-HP (par exemple les vols ou pertes de matériel, les vols ou pertes d'informations, ou les dysfonctionnements du poste de travail, un incident sur une application), ou toute violation des règles décrites dans le présent document, doivent être signalées au support SI ou à votre responsable hiérarchique, qui traiteront l'incident.

En outre, en cas d'accès accidentel à un site Internet illicite ou potentiellement dangereux (site corrompu ou susceptible d'être vecteur d'une infection virale), déconnectez-vous immédiatement du site et informez le support SI.

Une fois déclarés, les incidents sont traités par les services compétents en fonction de leur nature.

## **Art.8 Tracabilité, procédures de contrôle et sanctions**

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

Conformément à la réglementation, l'AP-HP 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 l'AP-HP 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 (métrologie du réseau) ;
- 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.

Cette surveillance consiste en une analyse des traces laissées par l'utilisateur à l'occasion de l'utilisation des outils mis à disposition. Les données collectées sont entre autres :

- 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'AP-HP ;
- La durée de la connexion (notamment pour l'accès Internet).

Ces données collectées sont archivées pendant 1 an, au-delà un archivage anonyme de deux ans, est conservé à des fins statistiques.

Les traitements informatiques portant sur ces données à caractère personnel font l'objet d'une déclaration normale auprès de la CNIL (Récépissé N°1562250 V1 daté du 26 mars 2012) conformément aux dispositions de la loi du 6 janvier 1978 modifiée.

Ainsi, l'AP-HP surveille et analyse les dispositifs professionnels dont :

- L'utilisation d'internet,
- L'utilisation de la messagerie électronique,
- L'utilisation des téléphones et télécopieurs,
- L'accès aux postes de travail et aux applications ainsi que les actions effectuées,
- Les accès aux répertoires partagés ou aux bases collaboratives.

L'AP-HP n'effectue aucun contrôle a priori de l'activité des utilisateurs.

Toutes les données, tous les messages électroniques, tous les SMS émis, reçus ou stockés sur le Système d'Information de l'AP-HP ou sur un matériel ou un système informatique fourni par l'AP-HP non identifiés comme étant personnels seront, par défaut, considérés comme étant professionnels.

De ce fait, chacun doit veiller à clairement identifier la nature personnelle d'un message ou d'une donnée en indiquant la mention « Privé » ou « Personnel » dans le titre de celui-ci ou en le stockant dans un répertoire portant cette même mention. De plus, l'utilisateur ne doit en aucun cas transformer ou qualifier des messages ou des données de nature professionnelle en messages ou données personnels.

En cas de risque particulier susceptible de porter préjudice à l'AP-HP, à l'un de ses agents ou à un tiers, dans l'un des cas visés par l'article 2.1 ou dans le cadre d'une enquête judiciaire, l'AP-HP pourra être amenée à consulter les traces nominatives et l'ensemble des données à caractère personnel des utilisateurs en présence du propriétaire des informations concernées ou celui-ci dûment prévenu.

En cas d'absence ou de départ de l'utilisateur, quel qu'en soit le motif, l'utilisateur doit s'organiser pour permettre à l'AP-HP d'accéder à tous les fichiers non classés sous les répertoires « mes données personnelles », ceux-ci étant présumés à caractère professionnel, qu'il a enregistré sur son poste ou sur le serveur de l'AP-HP, au besoin par la communication de ses mots de passe.

Pour assurer la continuité de son activité et en particulier la continuité de la prise en charge des patients, l'AP-HP pourra accéder aux informations professionnelles stockées dans le système d'information de l'AP-HP.

Les modalités d'accès par l'AP-HP aux informations médicales garantiront la préservation du respect du secret médical. Elles ne pourront avoir lieu qu'en présence du professionnel de santé dépositaire de l'information à caractère personnel relative à la santé après avoir été préalablement informé, à défaut de la présence du professionnel de santé, celle d'un représentant de la Commission Médicale d'Etablissement Locale ou Centrale.

Les modalités d'accès par l'AP-HP aux informations relatives aux activités universitaires garantiront la préservation du respect du secret professionnel. Elles ne pourront avoir lieu qu'en présence du professionnel dépositaire de l'information relative aux activités universitaires après avoir été préalablement informé, à défaut de la présence du professionnel, celle d'un représentant nommé par le Doyen de l'Université auquel le professionnel est rattaché.

L'accès par l'AP-HP aux informations liées aux activités syndicales ou à des activités de représentation (CME, CHSCT, CTE, ...) ne pourra avoir lieu qu'avec l'accord explicite et écrit de l'utilisateur concerné qui pourrait se faire assister par un représentant syndical de son choix ou un représentant de son choix, membre de l'instance à laquelle il appartient.



## 8.1 Sanctions

En cas de violation avérée des politiques et des règlements en vigueur dont les règles de la Charte d'utilisation du Système d'Information et conformément au règlement intérieur, l'AP-HP se réserve le droit d'entamer une procédure pour des mesures disciplinaires appropriées et proportionnelles aux actes (blâmes, avertissements, etc.) à l'encontre des agents concernés. Par ailleurs, l'AP-HP pourra procéder à la suspension des droits d'accès de l'utilisateur au SI après que ce dernier ait été mis à même de présenter ses observations. En cas de violation des règles définies en 2.1, le Directeur général de l'AP-HP pourra décider une suspension immédiate des droits d'accès à titre conservatoire. De plus, certaines violations pourront également faire l'objet de poursuites judiciaires.

En cas de suspension ou interruption des droits d'accès de l'utilisateur au SI, l'AP-HP permettra à l'utilisateur la récupération des données pendant un délai d'un mois dans le respect des règles de propriété des données.

Concernant les utilisateurs liés par un contrat de prestation ou une convention avec l'AP-HP, tels que les intérimaires, les partenaires ou les fournisseurs, toute violation des règles de bon usage du Système d'Information, pourra engendrer la rupture dudit contrat et des poursuites à l'égard de l'entreprise d'origine ou de la personne concernée.

## Art.9 Application de la charte d'utilisation du système d'information et publicité

Conformément à l'article L. 6143-7 du Code de la santé publique, le Directeur Général de l'AP-HP a arrêté la présente charte d'utilisation du Système d'Information après :

- Information de la commission centrale et des commissions locales des soins infirmiers, de rééducation et médicotéchniques, en date du 14 décembre 2015 ;
- Information des doyens des UFR de médecine de la Région Ile de France ;
- Consultation des instances représentatives centrales de l'Assistance Publique-Hôpitaux de Paris compétentes :
- Le comité d'hygiène, de sécurité et des conditions de travail central, lors de la séance du 22 septembre 2015 ;
- Le comité technique d'établissement central, lors de la séance du 5 octobre 2015 ;
- La commission médicale d'établissement, lors des séances du 12 mai 2015 ;
- Soumission pour avis au conseil de surveillance lors de la séance du 10 décembre 2015 ;
- Soumission pour concertation au Directoire lors de la séance du 17 novembre 2015 ;

Les présentes règles de la Charte d'utilisation du Système d'Information, annexe du règlement intérieur, ont été adressées au directeur général de l'agence régionale de santé après la tenue du conseil de surveillance du 10 décembre 2015.

La Charte d'utilisation du Système d'Information entre en vigueur à compter de la date de publication mentionnée sur la page de garde.

La Charte d'utilisation du Système d'Information est publiée sur le site Intranet de l'AP-HP.

La Charte d'utilisation du Système d'Information sera modifiée en fonction du contexte législatif et réglementaire.

Un rappel des textes juridiques fait l'objet de l'annexe 1.

Une règle de gestion des conditions d'accès et de sortie du Système d'Information lors de l'arrivée ou du départ des agents de l'AP-HP fait l'objet de l'annexe 2.

Un glossaire fait l'objet de l'annexe 3.

Toute modification du présent document sera notifiée aux utilisateurs par le biais du mailing, de la publication intranet et par voie d'affichage et selon la nature des modifications par une information (modification non substantielle) ou par un avis (modification substantielle) des instances représentatives centrales.

Pour toute question relative au document, la Direction des Systèmes d'Information, la Direction des Affaires Juridiques, le Responsable Sécurité du Système d'Information de votre entité ou de l'AP-HP peuvent être consultés.