UTILISER

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

XXX 2016

Version 2.0 – Validée – Diffusion Publique

ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

Sommaire

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 pour l'échange d'informations confidentielles avec vigilance.

PREAMBULE 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.

ARTICLE 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.

ARTICLE 2 : LES REGLES GENERALES 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 échant. 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.

ARTICLE 3 : SECURITE DES EQUIPEMENTS MIS A 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.

La connexion au SI d'équipements non fournis par l'AP-HP est soumise à des règles strictes.

La connexion, directe ou à distance notamment dans le cadre du télétravail, au réseau de l'AP-HP, d'équipements (postes de travail, tablettes, smartphone…) non fournis par la Direction des systèmes d'information, est soumise à autorisation formelle préalable et à des conditions d'intégration strictes. Si l'équipement autorisé devient non conforme par la suite, il sera déconnecté sans délai afin d'être remis en conformité. L'AP-HP n'assurera pas la maintenance de ces équipements.

Dès lors que ces équipements sont autorisés, ils sont soumis quant à leur gestion à l'application de la Charte informatique.

Les ordinateurs doivent être protégés physiquement.

Chacun doit veiller à utiliser les moyens de protection fournis par l'AP-HP tels que les câbles antivols 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.

ARTICLE 4 : DROIT D'ACCES 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.

ARTICLE 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).

ARTICLE 6 : UTILISATION DE LA MESSAGERIE ELECTRONIQUE

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.

ARTICLE 7 : REMONTEE DES INCIDENTS PAR LES UTILISATEURS

Toute 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.

ARTICLE 8 : TRAÇABILITE, PROCEDURES DE CONTROLE 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.

8.2 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.

ARTICLE 9 : APPLICATION DE LA CHARTE D'UTILISATION DU SYSTEME D'INFORMATION ET PUBLICITE

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 médicotechniques, 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.

Annexe 1 : Les principaux textes législatifs et réglementaires

La présente annexe de la charte informatique reprend les principaux textes législatifs et réglementaires concourant au droit applicable à l'utilisation du système d'information de l'AP-HP.

LE RESPECT DE LA CONFIDENTIALITE DES DONNEES DE SANTE

Le respect de la vie privée comprend toutes les dimensions du respect de l'intimité de la personne et de sa volonté. En ce qui concerne les informations, il ne se résume pas à la confidentialité. Il prend de nombreuses formes :

- Le droit de détenir des droits sur ses informations personnelles (donc de limiter les droits de ceux qui en ont connaissance) ;
- Le droit au secret des informations personnelles donc le droit de s'opposer aux traitements ou aux échanges ;

de celles-ci :

- Les droits dérivant des lois informatique et libertés : droit à l'information préalable, droit d'accès et de rectification, droit d'opposition, droit à l'oubli.

Le secret professionnel est régi par le code pénal (article 226-13) par les codes de déontologie à valeur réglementaire et par le code de santé publique (articles R.1112-7 et L.1110-4).

Article 226-13 du Code pénal

« 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 € d'amende. »

Code de déontologie médicale : Article R.4127-4 du CSP

« Le secret professionnel institué dans l'intérêt des patients s'impose à tout médecin dans les conditions établies par la loi.
Le secret couvre tout ce qui est venu à la connaissance du médecin 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. »

Au-delà, la loi n°2002-303 du 4 mars 2002 renforce, complète et précise le contenu du secret professionnel. Elle étend cette obligation à tous les professionnels de santé et plus généralement à tous les professionnels intervenant dans le système de santé.
Elle prévoit également des sanctions pour ceux qui tentent d'obtenir des informations en violation du secret professionnel.
Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique, comme leur transmission par voie électronique entre professionnels, sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés.
La carte de professionnel de santé et les dispositifs équivalents agréés sont utilisés par les professionnels de santé, les établissements de santé, les réseaux de santé ou tout autre organisme participant à la prévention et aux soins.
Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L. 1111-6 reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations.
Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès.

Article R. 1112-7 du CSP

« Les informations concernant la santé des patients sont soit conservées au sein des établissements de santé qui les ont constituées, soit déposées par ces établissements auprès d'un hébergeur agréé en application des dispositions à l'article L. 1111-8.
Le directeur de l'établissement veille à ce que toutes dispositions soient prises pour assurer la garde et la confidentialité des informations ainsi conservées ou hébergées. »

Article L1110-4 du CSP

« I.- Toute personne prise en charge par un professionnel de santé, un établissement ou un des services de santé définis au livre III de la sixième partie du présent code, un professionnel du secteur médico-social ou social ou un établissement ou service social et médico-social mentionné au I de l'article L. 312-1 du code de l'action sociale et des familles a droit au respect de sa vie privée et du secret des informations le concernant.
Excepté dans les cas de dérogation expressément prévus par la loi, ce secret couvre l'ensemble des informations concernant la personne venue à la connaissance du professionnel, de tout membre du personnel de ces établissements, services ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tous les professionnels intervenant dans le système de santé.
II.- Un professionnel peut échanger avec un ou plusieurs professionnels identifiés des informations relatives à une même personne prise en charge, à condition qu'ils participent tous à sa prise en charge et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins, à la prévention ou à son suivi médico-social et social.
III.- Lorsque ces professionnels appartiennent à la même équipe de soins, au sens de l'article L. 1110-12, ils peuvent partager les informations concernant une même personne qui sont strictement nécessaires à la coordination ou à la continuité des soins ou à son suivi médico-social et social. Ces informations sont réputées confiées par la personne à l'ensemble de l'équipe.
Le partage, entre des professionnels ne faisant pas partie de la même équipe de soins, d'informations nécessaires à la prise en charge d'une personne requiert son consentement préalable, recueilli par tout moyen, y compris de façon dématérialisée, dans des conditions définies par décret pris après avis de la Commission nationale de l'informatique et des libertés.
IV.- La personne est dûment informée de son droit d'exercer une opposition à l'échange et au partage d'informations la concernant. Elle peut exercer ce droit à tout moment. Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende.
V.- Le fait d'obtenir ou de tenter d'obtenir la communication de ces informations en violation du présent article est puni d'un an d'emprisonnement et de 15 000 euros d'amende.
En cas de diagnostic ou de pronostic grave, le secret médical ne s'oppose pas à ce que la famille, les proches de la personne malade ou la personne de confiance définie à l'article L. 1111-6 reçoivent les informations nécessaires destinées à leur permettre d'apporter un soutien direct à celle-ci, sauf opposition de sa part. Seul un médecin est habilité à délivrer, ou à faire délivrer sous sa responsabilité, ces informations.

Le secret médical ne fait pas obstacle à ce que les informations concernant une personne décédée soient délivrées à ses ayants droit, son concubin ou son partenaire lié par un pacte civil de solidarité, dans la mesure où elles leur sont nécessaires pour leur permettre de connaître les causes de la mort, de défendre la mémoire du défunt ou de faire valoir leurs droits, sauf volonté contraire exprimée par la personne avant son décès. Toutefois, en cas de décès d'une personne mineure, les titulaires de l'autorité parentale conservent leur droit d'accès à la totalité des informations médicales la concernant, à l'exception des éléments relatifs aux décisions médicales pour lesquelles la personne mineure, le cas échéant, s'est opposée à l'obtention de leur consentement dans les conditions définies aux articles L. 1111-5 et L. 1111-5-1.
VI.- Les conditions et les modalités de mise en œuvre du présent article pour ce qui concerne l'échange et le partage d'informations entre professionnels de santé et non-professionnels de santé du champ social et médico-social sont définies par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés. »

Article 57 de la Loi n°78-17 informatique et libertés

« Les personnes auprès desquelles sont recueillies des données à caractère personnel ou à propos desquelles de telles données sont transmises sont, avant le début du traitement de ces données, individuellement informées :

1. De la nature des informations transmises ;
2. De la finalité du traitement de données ;
3. Des personnes physiques ou morales destinataires des données ;
4. Du droit d'accès et de rectification institué aux articles 39 (droit d'accès) et 40 (droit de rectification) ;
5. Du droit d'opposition institué aux premier (opposition à la levée du secret professionnel) et troisième (refus de traitement après décès) alinéas de l'article 56 ou, dans le cas prévu au deuxième alinéa de cet article, de l'obligation de recueillir leur consentement.

Toutefois, ces informations peuvent ne pas être délivrées si, pour des raisons légitimes que le médecin traitant apprécie en conscience, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic grave. Dans le cas où les données ont été initialement recueillies pour un autre objet que le traitement, il peut être dérogé à l'obligation d'information individuelle lorsque celle-ci se heurte à la difficulté de retrouver les personnes concernées. Les dérogations à l'obligation d'informer les personnes de l'utilisation de données les concernant à des fins de recherche sont mentionnées dans le dossier de demande d'autorisation transmis à la Commission nationale de l'informatique et des libertés, qui statue sur ce point. »

Ce droit à l'information et au respect de la volonté ne s'oppose pas au droit à la protection vis-à-vis de cette même information. Il impose aux professionnels une réflexion et une appréciation en conscience pour rester en empathie des demandes du patient.

Décret confidentialité du 15 mai 2007 (R1110-1 du CSP)

Confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique

« Art. R. 1110-1. − Les professionnels participant à la prise en charge d'une même personne peuvent, en application de l'article L. 1110-4, échanger ou partager des informations relatives à la personne prise en charge dans la double limite :
1° Des seules informations strictement nécessaires à la coordination ou à la continuité des soins, à la prévention, ou au suivi médico-social et social de ladite personne ;
2° Du périmètre de leurs missions. »

« Art. R. 1110-2. Les professionnels susceptibles d'échanger ou de partager des informations relatives à la même personne prise en charge appartiennent aux deux catégories suivantes :

1° Les professionnels de santé mentionnés à la quatrième partie du présent code, quel que soit leur mode d'exercice ;
2° Les professionnels relevant des sous-catégories suivantes :
a) Assistants de service social mentionnés à l'article L. 411-1 du code de l'action sociale et des familles ;
b) Ostéopathes, chiropracteurs, psychologues et psychothérapeutes non professionnels de santé par ailleurs, aides médico-psychologiques et accompagnants éducatifs et sociaux ;
c) Assistants maternels et assistants familiaux mentionnés au titre II du livre IV du code de l'action sociale et des familles ;
d) Educateurs et aides familiaux, personnels pédagogiques occasionnels des accueils collectifs de mineurs, permanents des lieux de vie mentionnés au titre III du livre IV du même code ;
e) Particuliers accueillant des personnes âgées ou handicapées mentionnés au titre IV du livre IV du même code ;
f) Mandataires judiciaires à la protection des majeurs et délégués aux prestations familiales mentionnés au titre VII du livre IV du même code ;
g) Non-professionnels de santé salariés des établissements et services et lieux de vie et d'accueil mentionnés aux articles L. 312-1, L. 321-1 et L. 322-1 du même code, ou y exerçant à titre libéral en vertu d'une convention ;
h) Non-professionnels de santé mettant en œuvre la méthode prévue à l'article L. 113-3 du même code pour la prise en charge d'une personne âgée en perte d'autonomie ;
i) Non-professionnels de santé membres de l'équipe médico-sociale compétente pour l'instruction des demandes d'allocation personnalisée d'autonomie mentionnée aux articles L. 232-3 et L. 232-6 du même code, ou contribuant à cette instruction en vertu d'une convention. »

« Art. R. 1110-3. − I. — Le professionnel relevant d'une des catégories de l'article R. 1110-2 souhaitant échanger des informations relatives à une personne prise en charge, au titre du II de l'article L. 1110-4, avec un professionnel relevant de l'autre catégorie, informe préalablement la personne concernée, d'une part, de la nature des informations devant faire l'objet de l'échange, d'autre part, soit de l'identité du destinataire et de la catégorie dont il relève, soit de sa qualité au sein d'une structure précisément définie.
II. — Lorsqu'ils sont membres d'une même équipe de soins, les professionnels relevant d'une des catégories mentionnées à l'article R. 1110-2, partagent, avec ceux qui relèvent de l'autre catégorie, les informations relatives à une personne prise en charge dans les strictes limites de l'article R. 1110-1 et en informent préalablement la personne concernée. Ils tiennent compte, pour la mise en œuvre de ce partage, des recommandations élaborées par la Haute Autorité de santé avec le concours des ordres professionnels, en particulier pour ce qui concerne les catégories d'informations qui leur sont accessibles.
III. — Lorsque la personne est hors d'état d'exprimer sa volonté, seule l'urgence ou l'impossibilité d'informer cette personne peut dispenser le professionnel ou la personne participant à sa prise en charge de l'obligation d'information préalable. La personne concernée est toutefois informée, dès que son état de santé le permet, de l'échange ou du partage des informations auquel il a été procédé. Il en est fait mention dans le dossier médical. »

LE RESPECT DE LA DIGNITE ET DES BONNES MŒURS

Article 227-24 du Code Pénal

« Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.
Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

Article 227-23 du Code Pénal

« Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation.
Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.
Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.
Le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende.
Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 euros d'amende lorsqu'elles sont commises en bande organisée.
La tentative des délits prévus au présent article est punie des mêmes peines.
Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image. »

LA PROTECTION DES LIBERTES INDIVIDUELLES

Article 9 du Code civil

« Chacun a droit au respect de sa vie privée.
Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé. »

Article 226-16 du Code Pénal

« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Est puni des mêmes peines le fait de permettre l'accès aux données contenues dans un traitement mentionné à l'article L. 4123-9-1 du code de la défense sans avoir recueilli l'avis favorable mentionné au II du même article.».

Article 226-16-1 A du Code Pénal

Lorsqu'il a été procédé ou fait procéder à un traitement de données à caractère personnel dans les conditions prévues par le I ou le II de l'article 24 de la loi n° 78-17 du 6 janvier 1978 précitée, le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Article 226-16-1 du Code Pénal

« Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »

Article 226-17 du Code Pénal

« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi nº 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

Article 226-18 du Code Pénal

« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende ».

Article 226-19 du Code Pénal

« Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende .

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté ».

Article 226-19-1 du Code Pénal

« En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à un traitement :

1. Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci ;
2. Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant. »

Article 226-20 du Code Pénal

« Le fait de conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi.

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa ».

Article 226-21 du Code Pénal

« Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende ».

Article 226-22 du Code Pénal

« Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.
La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence.
Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit ».

Article 226-23 du Code Pénal

« Les dispositions de l'article 226-19 sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles ».

LE RESPECT DU DROIT DE LA PROPRIETE INTELLECTUELLE

Article L122-6 du Code de la Propriété Intellectuelle

« Sous réserve des dispositions de l'article L. 122-6-1, le droit d'exploitation appartenant à l'auteur d'un logiciel comprend le droit d'effectuer et d'autoriser :

1. La reproduction permanente ou provisoire d'un logiciel en tout ou partie par tout moyen et sous toute forme. Dans la mesure où le chargement, l'affichage, l'exécution, la transmission ou le stockage de ce logiciel nécessitent une reproduction, ces actes ne sont possibles qu'avec l'autorisation de l'auteur ;
2. La traduction, l'adaptation, l'arrangement ou toute autre modification d'un logiciel et la reproduction du logiciel en résultant ;
3. La mise sur le marché à titre onéreux ou gratuit, y compris la location, du ou des exemplaires d'un logiciel par tout procédé. Toutefois, la première vente d'un exemplaire d'un logiciel dans le territoire d'un Etat membre de la Communauté européenne ou d'un Etat partie à l'accord sur l'Espace économique européen par l'auteur ou avec son consentement épuise le droit de mise sur le marché de cet exemplaire dans tous les Etats membres à l'exception du droit d'autoriser la location ultérieure d'un exemplaire ».

Article L335-3 du Code de la Propriété Intellectuelle

« Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi. Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article L. 1226 ».

Article L335-2 du Code de la Propriété Intellectuelle

« Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.
Seront punis des mêmes peines le débit, l'exportation, l'importation, le transbordement ou la détention aux fins précitées des ouvrages contrefaisants.
Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende. »

LE RESPECT DE L'INTEGRITE D'UN SYSTEME INFORMATIQUE

Article 323-1 du Code Pénal

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.
Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

Article 323-2 du Code Pénal

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende ».

Article 323-3 du Code Pénal

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.
Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

Article 323-5 du Code Pénal

« Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes :

1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ;
2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ;
3. La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;
5. L'exclusion, pour une durée de cinq ans au plus, des marchés publics ;
6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35 ».

LE RESPECT DU SECRET DE LA CORRESPONDANCE ECHANGEE PAR LE CANAL INFORMATIQUE

Article 226-4-1 du Code Pénal

« Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.
Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne. »

Article 226-15 du Code Pénal

« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions ».

Article 432-9 du Code Pénal

« Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45 000 euros d'amende.
Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu ».

LE DEPOT LEGAL DES LOGICIELS ET DES BASES DE DONNEES

Article L 131-2 du Code du Patrimoine

« Les documents imprimés, graphiques, photographiques, sonores, audiovisuels, multimédias, quel que soit leur procédé technique de production, d'édition ou de diffusion, font l'objet d'un dépôt obligatoire, dénommé dépôt légal, dès lors qu'ils sont mis à la disposition d'un public. Toutefois, les documents destinés à une première exploitation en salles de spectacles cinématographiques sont soumis à l'obligation de dépôt légal dès lors qu'ils ont obtenu le visa d'exploitation cinématographique prévu à l'article L. 211-1 du code du cinéma et de l'image animée.
Les logiciels et les bases de données sont soumis à l'obligation de dépôt légal dès lors qu'ils sont mis à disposition d'un public par la diffusion d'un support matériel, quelle que soit la nature de ce support.
Sont également soumis au dépôt légal les signes, signaux, écrits, images, sons ou messages de toute nature faisant l'objet d'une communication au public par voie électronique. »

Article L 133-1 du Code du Patrimoine

« Le fait, pour toute personne mentionnée à l'article L. 132-2, de se soustraire volontairement à l'obligation de dépôt légal est puni d'une amende de 75 000 euros. La juridiction répressive peut, après avoir déclaré le prévenu coupable, ajourner le prononcé de la peine en lui enjoignant, sous astreinte le cas échéant, de se conformer, dans un délai fixé, aux prescriptions qu'elle détermine et qui ont pour objet de faire cesser l'agissement illicite et d'en réparer les conséquences.

Dans le cas où la juridiction répressive assortit l'ajournement d'une astreinte, elle doit prévoir le taux et la date à compter de laquelle cette astreinte commencera à courir. L'ajournement, qui ne peut intervenir qu'une seule fois, peut être décidé même si le prévenu ne comparaît pas en personne.

Le juge peut ordonner l'exécution provisoire de la décision d'injonction.

A l'audience de renvoi, qui doit intervenir au plus tard dans le délai d'un an à compter de la décision d'ajournement, la juridiction statue sur la peine et liquide l'astreinte s'il y a lieu. Elle peut, le cas échéant, supprimer cette dernière ou en réduire le montant. L'astreinte est recouvrée par le comptable public compétent comme une amende pénale. Elle ne peut donner lieu à contrainte judiciaire. »

Annexe 2 : Règles de gestion pour l’accès des agents au Système d’Information

Contexte

Les agents de l’AP-HP qui en ont la nécessité accèdent au SI de l’AP-HP. Cette fiche décrit les règles d’accès au SI de l’AP-HP et la gestion du départ de ses collaborateurs. Elle est une annexe à la charte informatique.

LES OUTILS

Chaque personnel est identifié par son matricule : APH suivi de 7 chiffres (ex : APH0012345).
Pour chaque personnel, un code de position **statutaire** est indiqué, ainsi que plusieurs codes associés. Ces codes sont en annexe de cette note.

L’AP-HP a mis en place un annuaire technique, ACTIVE DIRECTORY (AD), qui permet de centraliser des informations relatives aux utilisateurs et aux ressources informatiques de l’AP-HP en fournissant des mécanismes d’identification et d’authentification, tout en sécurisant l’accès aux données.

La mise à jour de l’AD se fait à partir de HRAccess en tenant compte de la position statutaire de l’agent. Les agents de l’AP-HP sont gérés administrativement dans l’application informatique HRAccess.

Règles générales de gestion

Tout agent en position statutaire AC (activité) a potentiellement accès au système d’information.
Les habilitations aux différentes applications sont demandées par le supérieur hiérarchique en fonction des nécessités de service.
Pour toutes les autres positions statutaires, les accès aux applications sont désactivés le lendemain de la date du départ saisie dans HRAccess, puis supprimés automatiquement un an après.
Les règles de désactivation du compte de messagerie sont décrites ci-dessous.
Les agents en cumul emploi retraite sont en position statutaire d’activité (AC). De fait, ils conservent leur code APH salarié AP-HP, l’accès aux applications et leur adresse de messagerie AP-HP.
Les départs à la retraite : Une désactivation préalable peut être faite à la demande du responsable de l’agent (période de prise de CA ou RT).
Ces règles seront mises en œuvre dans le paramétrage de la solution informatique de Gestion des Identités et des Accès (IAM). Elles s’appliqueront à la date de diffusion au sein de l’AP-HP de la solution IAM pour retirer l’accès aux applications et à la messagerie.

Règles de gestion du Personnel Médical

Annexe 2 : Règles de gestion pour l'accès des agents au Système d'Information

On entend par Personnel Médical : les médecins, les pharmaciens, les chirurgiens-dentistes et les sages-femmes travaillant à l'AP-HP.

La messagerie :

> Le compte de messagerie de l'utilisateur sera désactivé **2 mois** après la date du départ saisie dans HRAccess, puis supprimé automatiquement un an après.

Les cas d'exceptions :

- Les personnels médicaux, ayant quitté l'AP-HP et qui contribuent aux missions d'Enseignement, de Recherche, de Référence et d'Innovation (MERRI), auront un nouvel identifiant (APH en 7 xxx xxx) pour accéder à leur adresse de messagerie AP-HP et aux applications. La demande devra être faite par le chef de service auprès du bureau de gestion du personnel médical en lien avec la direction du GH/sites/PIC et la DSI locale.
- Les autres demandes d'exception sont remontées au cabinet du secrétariat général de l'AP-HP pour traitement.

Règles de gestion du Personnel non médical

La messagerie :

> Le compte de messagerie de l'utilisateur sera désactivé **1 mois** après la date du départ saisie dans HRAccess, puis supprimé automatiquement un an après.

Les cas d'exceptions :

- Les agents AP-HP, mis à disposition et assurant des gardes, conservent leurs accès au système d'information via les moyens d'accès actuellement autorisés à l'AP-HP. Ces cas seront traités par les Directions des GH/Sites/PIC et la DSI locale.
- Les autres demandes d'exception sont remontées au cabinet du secrétariat général de l'AP-HP pour traitement.

Annexe 2 : Règles de gestion pour l'accès des agents au Système d'Information

Liste des Codes « Position Statutaire » dans HRACCESS

Code	Libellé long	Code-Position statutaire	Position statutaire	Code-Catégorie de situation	Code-Motif	Motif
ACTI	Activité	AC	ACTIVITE	ACTIVE	ERP	ENTREE REPRISE
ACTPRO	Prolongation d'activité	AC	ACTIVITE	ACTIVE	ENT	Entrée
CAD	Congé d'adoption	AC	ACTIVITE	NONPRE	CGD	Congés divers
CMA	Congé de maternité	AC	ACTIVITE	NONPRE	CGD	Congés divers
CPR	Congé de paternité	AC	ACTIVITE	NONPRE	CGD	Congés divers
INVAL	Assur Inval	AC	ACTIVITE	NONPRE	INV	Assur inval
IRN	Stage inter région non rémunéré	AC	ACTIVITE	ACTIVE	ENT	Entrée
LAB	Stage laboratoire (interne résident)	AC	ACTIVITE	ACTIVE	ENT	Entrée
MADE	Mise à disposition entrante	AC	ACTIVITE	ACTIVE	MAE	MAD entrant
MADEF	Mise à disposition MADEF	AC	ACTIVITE	NONPRE	MAS	MAD sortant
MAFONC	Maintien en fonction	AC	ACTIVITE	ACTIVE	ENT	Entrée
MIT	Mission temporaire	AC	ACTIVITE	NONPRE	MIS	Mission
OFF1	Congé spécial	AC	ACTIVITE	NONPRE	CGD	Congés divers
PRA	Stage chez un praticien (interne résident)	AC	ACTIVITE	ACTIVE	ENT	Entrée
QUH	Quadrimestre hors A.P. - Etudiant	AC	ACTIVITE	ACTIVE	ENT	Entrée
RECLIM	Recul limite d'âge	AC	ACTIVITE	ACTIVE	ENT	Entrée
SDT	Stage inter region DOM-TOM (interne)	AC	ACTIVITE	ACTIVE	ENT	Entrée
SIR	Stage inter région (interne)	AC	ACTIVITE	ACTIVE	ENT	Entrée
CEN1	Congés contr pr créer ou reprendre entreprise	NR	CONGE NON REMUNERE	NONPRE	CGD	Congés divers
CPE2	Congés contractuels pour convenances perso.	NR	CONGE NON REMUNERE	NONPRE	CGD	Congés divers
ENF2	Congés contractuels pour élever un enfant	NR	CONGE NON REMUNERE	NONPRE	CGD	Congés divers
FNT1	Congés contractuels fonctions parlementaires	NR	CONGE NON REMUNERE	NONPRE	CGD	Congés divers
MIT3	Mission temporaire non rémunérée	NR	CONGE NON REMUNERE	NONPRE	MIS	Mission
ENF4	Congé parental	CP	CONGE PARENTAL	NONPRE	CGD	Congés divers
CFP0	Congé de formation non rémunéré	ST	CONGE SANS TRAITEM	NONPRE	CGD	Congés divers
CNJ1	Congés stagiaires pour suivre son conjoint	ST	CONGE SANS TRAITEM	NONPRE	CGD	Congés divers
CST	Congé sans traitement	ST	CONGE SANS TRAITEM	NONPRE	CGD	Congés divers
ENF3	Congé stagiaire parental pr élever un enfant	ST	CONGE SANS TRAITEM	NONPRE	CGD	Congés divers
SOI1	Congés stagiaire soins à conj, enf ou ascend	ST	CONGE SANS TRAITEM	NONPRE	CGD	Congés divers
DET	Détachement hors AP-HP	DE	DETACHEMENT	NONPRE	DES	Sortie en détachem
DOF	Détachement d'office	DE	DETACHEMENT	NONPRE	DES	Sortie en détachem
AOI	Dispo pour activité org. Intern. / Entreprise	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
ARN	Dispo année recherche (reprise par défaut)	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
CEN2	Dispo pour créer ou reprendre une entreprise	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
CNJ2	Disponibilité pour suivre son conjoint	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
CPE1	Disponibilité pour convenances personnelles	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
DEA	Disponibilité pour préparation DEA (interne)	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
DM2	Dispo d'off Sécurité sociale invalidité tx 50	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
DM3	Dispo d'off Sécurité sociale invalidité tx 70	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
ENF1	Disponibilité pour élever un enfant	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
ERG	Dispo pour études ou rech. d'intérêt général	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
FHF	Disponibilité pour préparation FHF (interne)	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
FOR	Disponibilité pour formation	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
MAND	Disponibilité mandat d'élu	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
OFF2	Disponibilité d'office	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
PRF	Disponibilité pour stage formation /perfect.	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
REPR	Toutes disponibilités	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
SOI2	Dispo soins à conjoint, enfant ou ascendant	DI	DISPONIBILITE	NONPRE	DIS	Disponibilité
OIN1	Hors cadre (orga international-mission coop)	HC	HORS CADRES	NONPRE	MIS	Mission
SCN	Hors cadre (Emploi sans pension CNRACL)	HC	HORS CADRES	NONPRE	HCA	Hors cadre
H032	Mise à disposition d'administration d'Etat-PM	MD	MISE A DISPOSITION	NONPRE	MAS	MAD sortant
H092	Mise à disposition etb public de l'Etat	MD	MISE A DISPOSITION	NONPRE	MAS	MAD sortant
MAD	Mise à disposition	MD	MISE A DISPOSITION	NONPRE	MAS	MAD sortant
N082	Mise à dispo dans organisme d'intérêt public	MD	MISE A DISPOSITION	NONPRE	MAS	MAD sortant
AIR	Absence irrégulière	NP	NON PAYE	NONPRE	AIR	Absence irrégulièr
DEL	Délégation	NP	NON PAYE	NONPRE	MIS	Mission
ETE	Exclusion temporaire	NP	NON PAYE	NONPRE	EXT	Exclusion temporai
FINAC	Sortie définitive en cours de mois	NP	NON PAYE	NONPRE	SOR	Sortie
GRE	Absence de service non fait	NP	NON PAYE	NONPRE	GRE	Grève
N062	Position spéciale pour mission à l'étranger	NP	NON PAYE	NONPRE	MIS	Mission
STE	Stage à l'étranger ou mission humanitaire	NP	NON PAYE	NONPRE	SOR	Sortie
CFA1	Congé fin d'activité non titulaire (Reprise)	NS	NON STATUTAIRE	NONPRE	CGD	Congés divers
CFA2	Congé fin d'activité personnel médical	NS	NON STATUTAIRE	NONPRE	CGD	Congés divers
CFA3	Congé fin d'activité titulaire (Reprise)	NS	NON STATUTAIRE	NONPRE	CGD	Congés divers
COO	Coopération	SN	SERVICE NATIONAL	NONPRE	SEN	Service national
OBJ	Objecteur de conscience (reprise)	SN	SERVICE NATIONAL	NONPRE	SOR	Sortie
PMR	PERIODE MILITAIRE REMUNEREE	SN	SERVICE NATIONAL	NONPRE	SEN	Service national
PNR	PERIODE MILITAIRE NON REMUNEREE	SN	SERVICE NATIONAL	NONPRE	SEN	Service national
RES	Service national et reserves op. et sanitaire	SN	SERVICE NATIONAL	NONPRE	SEN	Service national

Annexe 3 : Glossaire

Archivage : Action de recueillir, de classer et de conserver des documents à des fins de consultation ultérieure.

Authentifiant : Attribut permettant de vérifier que l'accédant qui souhaite se connecter à un système est bien celui qu'il prétend être. Il s'agit généralement d'un mot de passe.

Bien : Élément unitaire (logiciel, matériel, service) pour lequel s'applique les règles de bon usage du Système d'Information.

Cheval de Troie : *TROJAN* en anglais. Programme malveillant qui se masque en un programme favorable. Sa particularité par rapport à d'autres codes malveillants est qu'il ne se multiplie pas. Il peut notamment offrir à un attaquant :

- Un accès complet au système,
- Des informations de types mots de passe ou adresse de messagerie,
- La liste de toutes les actions exercées par l'utilisateur.

Chiffrement (appelé aussi improprement "cryptage") : Moyen à utiliser pour préserver la confidentialité des informations sous forme électronique. Le contenu d'un message, d'un document, est alors rendu illisible pour quiconque ne possède pas la clé permettant de le déchiffrer.

CNIL : Commission Nationale de l'Informatique et des Libertés. Autorité administrative indépendante chargée de veiller au respect de la vie privée et des libertés dans le monde numérique.

Code PIN : Numéro d'identification personnel composé de plusieurs chiffres permettant d'authentifier le propriétaire d'une ressource (téléphone portable, carte de paiement, etc.).

Compte : Ensemble des éléments d'une connexion à une ressource, permettant à son titulaire d'utiliser ladite ressource. Il s'agit généralement d'un identifiant, d'un authentifiant, et des droits associés.

Confidentialité : Un des critères de sécurité permettant de s'assurer que l'information ne soit accessible qu'aux personnes autorisées à y accéder.

Contrôle d'accès : Fonctionnalité de sécurité visant à autoriser l'accès à un bien ou un traitement en fonction de l'identifiant et l'authentifiant fournis et des droits associés.

Disponibilité : Un des critères de sécurité, aptitude d'une fonction à rendre le service attendu en temps voulu et dans les conditions d'usage prévues.

Droits d'accès : Ensemble de droits accordés sur une ressource, permettant d'effectuer des actions sur celle-ci (création, consultation, modification, suppression).

Fraude informatique : Toute conduite qui implique la manipulation d'un ordinateur ou des informations informatiques, quelle que soit la méthode utilisée, dans le but d'obtenir de façon malhonnête de l'information, de l'argent, des biens ou tout autre avantage, ou dans l'intention de nuire (ex : captation ou suppression d'informations, copie pirate de logiciels ; accès, entrave ou altération d'un traitement automatisé des informations…).

Gestion Technique centralisée ou GTC est un mode de supervision par système d'automate centralisé, gérant un très grand nombre de paramètres et de fonctions différentes, à partir des données envoyées par des capteurs au sein de grandes structures.

Habilitation : Attribution à un utilisateur de droits d'accès à des biens informatiques par une entité autorisée.

Identifiant : *Login* en anglais. Attribut unique permettant à une personne de s'identifier à un système. Il s'agit, à titre d'illustration, du code APH pour les agents. Il est généralement associé à un authentifiant.

Annexe 3 : Glossaire

Incidents de sécurité : on appelle incident de sécurité du Système d'Information tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité du Système d'Information de l'AP-HP. Il peut s'agir de vol d'information, de corruption de données, ou d'infection virale d'un poste de travail par exemple.

Informations à caractère personnel : Toute information relative à une personne physique identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (art. 2 de la loi du 6 janvier 1978 modifiée en août 2004).

Intégrité : Un des critères de sécurité, garantie de l'exactitude, de la fiabilité et de l'exhaustivité des informations et des méthodes de traitement.

Nom de domaine ou adresse URL : Correspond à l'adresse d'un site Internet. Il est composé deux parties : le nom du site et un suffixe tel que « .fr », « .org », etc.

Pare-feu : *Firewall* en anglais. Outil matériel ou logiciel permettant de définir les typologies de communications autorisées sur un réseau.

Partenaire : Entité externe qui intervient en liaison avec l'AP-HP sur un domaine donné (exemple : les associations).

Pourriel : Le pourriel (SPAM) est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

Responsable de la Sécurité du Système d'Information (RSSI) : Il assure la gouvernance et le pilotage de la sécurité à l'échelle de son entité en identifiant les risques, porte les projets de sécurité, et apporte un support concernant les problématiques de sécurité. Le rôle des RSSI est défini dans la Politique Générale de Sécurité du SI de l'AP-HP.

Sous-traitant : Cf. loi n°75-1334 du 31 décembre 1975 relative à la sous-traitance.

Spam : cf. pourriel.

Support SI : Service à contacter pour toute question relative au Système d'Information. Il peut s'agir du support SI des Groupes Hospitaliers, des sites ou des CCS pour tout ce qui concerne les applications.

Système d'Information : ensemble organisé de ressources (données, procédures, matériels, logiciels, personnels, etc.) permettant d'acquérir, traiter, stocker, diffuser ou détruire les informations utilisées par les entités dans leurs métiers, et ceci quel que soit le support des informations.

Tiers : Entités ou organismes externes à la relation contractuelle entre le Titulaire avec l'AP-HP. Sont ainsi considérés comme des tiers : les prestataires, les intérimaires, les partenaires, les sous-traitants…

Traçabilité : critère de sécurité qui garantit le suivi des actions des utilisateurs lors de l'utilisation ou de l'accès aux ressources matérielles ou informatiques.

Utilisateur : Désigne toute personne susceptible de pouvoir accéder au SI de l'AP-HP. Sauf mention contraire, désigne également les administrateurs, les exploitants et les prestataires externes intervenant sur le SI.

Ver : Programme autonome dont la vocation première est de se répliquer. Il intègre ses propres fonctions de réplication et d'infection. Il peut ainsi se transmettre en tant que pièce jointe à un courrier électronique (« mass-mailer »), ou se propager *via* le réseau.

VPN ou Virtual Private Network : Il s'agit d'un réseau privé virtuel mis en place par les organismes souhaitant interconnecter leur réseau à celui d'un organisme tiers. Le VPN peut être considéré comme une extension du réseau permettant de préserver le niveau de sécurité de celui-ci.

Virus : Programme hostile susceptible d'infecter les fichiers, de saturer les réseaux. Il peut en résulter des dysfonctionnements divers : par exemple l'effacement du disque dur, la suppression ou la compromission de fichiers.

Annexe 3 : Glossaire

WIFI : Ensemble de protocoles de communication sans fils permettant de faire communiquer plusieurs équipements informatiques.