ASSISTANCE PUBLIQUE HÔPITAUX DE PARIS

www.aphp.fr

Charte informatique de l'AP-HP
07/01/2022
DSI

Synthèse :

La disponibilité, la sécurité, la confidentialité et le bon fonctionnement du système d'information de l'AP-HP revêtent un caractère stratégique pour l'ensemble de ses membres et de ses patients. La continuité de l'activité dépend d'une utilisation raisonnée des ressources informatiques mises à disposition des Utilisateurs.

L'accès aux ressources informatiques de l'AP-HP peut présenter des risques en cas d'utilisation non conforme (atteinte à l'image de l'AP-HP, divulgation d'informations confidentielles, violation de données personnelles). La réalisation de ces risques peut engager la responsabilité civile et/ou pénale de l'AP-HP et des Utilisateurs fautifs.

Afin de se prémunir au mieux contre ces risques, l'Utilisateur doit respecter, lorsqu'il accède à ces ressources ou qu'il les utilise, un certain nombre de règles, notamment :

- Les règles de confidentialité, notamment s'agissant du respect du secret médical :
  - L'accès au dossier d'un patient n'est autorisé qu'aux professionnels faisant partie de l'équipe de soin ayant pris en charge ledit patient : tout autre accès est illégitime
  - L'Utilisateur ne doit pas tenter d'accéder à des dossiers pour lesquels il n'est pas habilité, et même s'il est habilité, il ne doit accéder qu'aux seuls dossiers strictement nécessaires à sa mission
  - L'utilisation d'une messagerie sécurisée est obligatoire pour tout échange de données de santé avec d'autres professionnels de santé en dehors de l'AP-HP
  - Les données personnelles doivent être stockées dans des espaces sécurisés, leur collecte limitée à ce qui est strictement nécessaire et leur durée de conservation limitée ;

- Les règles de sécurité physiques et logiques, visant à préserver la pérennité du SI de l'AP-HP :
  - Les moyens d'authentification sont personnels, confidentiels et non transmissibles
  - Les ressources confiées aux Utilisateurs doivent être protégées physiquement et logiquement
  - Les ressources doivent être utilisées à des fins professionnelles ; l'utilisation à titre personnel est tolérée, mais de manière raisonnable
  - La configuration initiale du poste de travail doit être conservée car elle a été étudiée afin de garantir le bon fonctionnement et la sécurité du SI
  - La connexion au SI de ressources non fournies par l'AP-HP suppose l'accord préalable de la DSI
  - Il est par principe interdit d'utiliser des réseaux publics wifi non sécurisés
  - Les données nécessaires à la continuité de l'activité de l'AP-HP doivent être sauvegardées
  - Toutes les actions des Utilisateurs sur le SI de l'AP-HP sont tracées et pourront être auditées

- Les règles d'éthique, de courtoisie et de professionnalisme, applicables en toutes circonstances :
  - Le devoir de réserve, la probité, la loyauté et la confidentialité s'appliquent en toutes circonstances
  - L'Utilisateur doit faire preuve de politesse et de respect à l'égard de ses interlocuteurs
  - Il est interdit de nuire à l'image de marque de l'AP-HP, à ses intérêts ou à sa réputation, de quelque manière que ce soit (par son comportement ou ses propos, notamment publiés sur des réseaux sociaux)

DRAFT

Toute violation de la Charte pourra faire l'objet de sanctions disciplinaires, contractuelles et/ou pénales. Des audits ciblés et/ou aléatoires sont menés périodiquement afin de contrôler les accès et usages des ressources, particulièrement s'agissant des accès aux dossiers patients informatisés.

DRAFT

Sommaire

1. Objet 4

2. Accès aux Ressources 4

2.1. Moyens d'authentification et mots de passe 4

2.2. Accès aux logiciels gérant des Données personnelles 5

2.3. Accès privilégiés des Utilisateurs de la DSI 7

3. Usage des Ressources 7

3.1. Usage professionnel et raisonné des Ressources 7

3.2. Utilisation du poste de travail 8

3.3. Utilisation de la messagerie professionnelle 9

3.4. Utilisation d'internet et d'intranet 9

3.5. Utilisation du téléphone 10

3.6. Utilisation des espaces de stockage 11

3.7. Utilisation des supports amovibles et imprimantes 11

3.8. Utilisation de Ressources personnelles 12

4. Traçabilité, contrôle et audits 12

4.1. Traçabilité et contrôle 12

4.2. Accès par l'AP-HP aux Ressources de l'Utilisateur 13

4.3. Audits réalisés afin de prévenir et sanctionner les accès illégitimes (violation du secret) 14

4.4. Remontée des incidents 14

5. Sanctions 14

6. Entrée en vigueur et procédure 15

7. Annexes 16

Annexe 1 : Définitions 17

Annexe 2 : Référentiel légal 18

DRAFT

1. Objet

La présente Charte a pour objet :

- De préciser les principaux droits, les devoirs et les responsabilités des Utilisateurs dans le cadre de l'accès et de l'utilisation des Ressources mises à disposition par l'AP-HP ;

- De faire prendre conscience à chaque Utilisateur de l'importance de la sécurité des Ressources, de le responsabiliser sur les règles de confidentialité et de secret professionnel et de l'alerter sur les sanctions encourues en cas de non-respect des règles.

La présente Charte s'inscrit dans le cadre de la Politique Générale de Sécurité du Système d'Information (PGSSI) de l'AP-HP, est validée par la Direction Générale après information, consultation et avis des instances compétentes visées à l'article « Entrée en vigueur et procédure ». Elle s'applique en complément des règles et politiques existantes de l'AP-HP consultables en permanence sur l'Intranet (ex. Politique de Sécurité Globale, charte sur le télétravail, charte sur l'EDS, charte d'utilisation des téléphones mobiles, etc.).

La présente Charte constitue une annexe du règlement intérieur de l'AP-HP. Toute violation fera l'objet de sanctions disciplinaires, contractuelles et/ou pénales. Des audits ciblés et/ou aléatoires sont menées périodiquement afin de contrôler les accès et usages des Ressources, particulièrement s'agissant des accès aux dossiers patients informatisés.

En cas de doute, ou pour toute question, l'Utilisateur est invité à s'adresser à son supérieur hiérarchique, et s'agissant des partenaires externes à l'AP-HP, au porteur du projet interne à l'AP-HP.

Le référentiel légal et les définitions des termes en majuscule utilisés dans la présente charte figurent en annexe 1 et 2.

2. Accès aux Ressources

Synthèse :

- *Les moyens d'authentification sont personnels, confidentiels et non transmissibles ;*
- *Le fait d'utiliser les moyens d'authentification d'un tiers, même avec son accord, est interdit, l'Utilisateur étant seul responsable de leur confidentialité et usage ;*
- *Les mots de passe doivent respecter les règles édictées par la DSI et être changés régulièrement ;*
- *L'accès aux informations se fait au regard des nécessités professionnelles pour l'exercice de l'activité de chaque Utilisateur ;*
- *L'accès au dossier d'un patient n'est autorisé qu'au professionnel de santé faisant partie de l'équipe de soin ayant pris en charge ledit patient. L'accès au dossier de ressources humaines d'un Utilisateur n'est autorisé ponctuellement qu'au professionnel habilité pour les besoins de ses missions. Tout autre accès est considéré comme illégitime et pourra faire l'objet d'une convocation de l'Utilisateur fautif puis l'application de sanctions disciplinaires, contractuelles et pénales ;*
- *Les Données personnelles sont soumises à une réglementation contraignante : l'accès et l'utilisation des Données personnelles ou encore la création d'un traitement de Données personnelles doit se faire dans le respect des principes de finalité, de transparence, de confidentialité, de sécurité, de minimisation, de proportionnalité et de pertinence.*

2.1. Moyens d'authentification et mots de passe

L'accès aux Ressources est géré par la DSI, seule habilitée à délivrer les moyens d'authentification (identifiant et mot de passe) à chaque Utilisateur, selon les procédures d'autorisation en vigueur et au regard de ses missions.

DRAFT

L'accès aux Ressources se décide au regard des nécessités professionnelles de chaque Utilisateur. Lorsqu'un Utilisateur estime qu'il ne dispose pas des habilitations adaptées au bon exercice de ses activités professionnelles, il doit s'adresser à son responsable hiérarchique afin de les faire modifier.

Les moyens d'authentification sont personnels, confidentiels et non transmissibles, l'Utilisateur étant seul responsable de leur confidentialité et usage. Les utilisations faites à l'aide d'un moyen d'authentification propre à chaque Utilisateur sont réputées être le fait du détenteur de ce moyen d'authentification, sauf à ce que sa bonne foi puisse être démontrée.

Il est notamment interdit :

- De communiquer ses identifiants et mots de passe à un tiers :
    - Risque d'erreur médicale ou d'accident de soin commis au nom du porteur des identifiants
    - Risque de perte de traçabilité précise des actes de soin effectués
- D'utiliser les identifiants et les mots de passe d'un tiers :
    - Usurpation d'identité (infraction pénale)
    - Introduction frauduleuse dans un Système de Traitement Automatisé de Données

L'accès de l'Utilisateur aux Ressources pourra être suspendu, supprimé, limité ou réexaminé, pour des raisons de sécurité et le cas échéant sans préavis, notamment :

- Lors de la cessation de son activité professionnelle au sein de son service (changement de service, mutation, etc…) ou en cas de départ, conformément à la procédure applicable dédiée à cet effet ;
- Dans certains cas de cessation temporaire de l'activité professionnelle (maladie, congé de maternité, etc. : dans ces cas, l'Utilisateur doit s'organiser pour permettre à l'AP-HP d'accéder aux données professionnelles pour assurer la continuité d'activité) ;
- Dès lors qu'un usage abusif sera révélé (et ce, sans préjudice des actions disciplinaires et pénales pouvant être initiées par l'AP-HP ou tout autre personne ayant subi un préjudice), par exemple :
    - En cas d'utilisation de moyens d'authentification autres que les siens ;
    - En cas d'utilisation en contradiction avec les règles professionnelles applicables, notamment s'agissant du secret médical ;
    - Plus généralement en cas manquement à la Charte ou de manquement aux lois et réglementations en vigueur.

Le supérieur hiérarchique s'assure de manière périodique que les droits d'accès accordés aux Utilisateurs sous sa responsabilité correspondent précisément à leurs rôles et missions. Il notifie à la DSI dans les meilleurs délais toute habilitation excessive qui dépasserait les besoins de l'Utilisateurs au regard de ses fonctions.

L'utilisation de comptes non personnels (par exemple les comptes génériques ou les comptes partagés) doit rester exceptionnelle et justifiée. 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.

S'agissant du mot de passe, l'Utilisateur doit se conformer aux préconisations de la DSI :

- Définir un mot de passe complexe (au moins 8 caractères et comportant majuscules, minuscules, chiffres) ;
- Veiller à le modifier régulièrement afin d'éviter toute usurpation de son identité ;
- Alerter sans délai le RSSI en cas de suspicion de compromission d'un moyen d'authentification.

Exemples de comportements abusifs et/ou sanctionnables :

- *Inscrire ses mots de passe sur support papier ou électronique à proximité des Ressources ou sur celles-ci, ou les stocker en clair dans un fichier ;*
- *Se connecter au dossier patient avec le compte d'un tiers, même avec son accord ;*
- *Ne jamais modifier le mot de passe, ou supprimer le mot de passe.*

2.2. Accès aux logiciels gérant des Données personnelles

DRAFT

Certains Utilisateurs disposent d'accès aux applications métiers traitant des Données personnelles et des Données de santé (ex. : HR Access, Orbis, DxCare,…), afin d'assurer la prise en charge des patients, ou encore dans le cadre de la gestion des ressources humaines.

La consultation frauduleuse ou la divulgation à des tiers de ces Données pourrait avoir un impact irrémédiable sur le patient ou sur un autre Utilisateur. Les Utilisateurs sont donc soumis au secret le plus absolu sur ces données confidentielles protégées par la loi et dont la collecte, l'utilisation, la consultation, le stockage ou encore l'échange est strictement encadré par des mesures de confidentialité et de sécurité.

S'agissant précisément de l'accès aux Données de santé, sont soumis au secret médical tous les Utilisateurs participant à la prise en charge des patients (ex. professions médicales, paramédicales, personnels administratifs, sociaux) qui ont accès à des Données personnelles de santé dans le cadre de leurs fonctions. Les conditions suivantes pour accéder aux dossiers patients doivent être impérativement respectées par ces Utilisateurs, sous peine de sanctions :

- Seuls peuvent accéder au dossier médical d'un patient les professionnels concourant directement à la prise en charge du patient, c'est-à-dire faisant partie de l'équipe de soin au sens de l'article L1110-12 du code de la santé publique ;
- Ces professionnels ne peuvent accéder qu'aux seules Données du patient concerné, dans la mesure où cela est strictement nécessaire à l'exécution de leurs missions.

Accéder au dossier d'un patient en dehors du cadre ci-dessus est constitutif d'une violation du secret médical, d'une atteinte à la vie privée des patients et susceptible de faire l'objet d'un recours contentieux du patient, contre l'Utilisateur fautif et contre l'AP-HP.

Les Utilisateurs soumis au secret ne doivent pas tenter de contourner les dispositifs de sécurité ni accéder, ou tenter d'accéder, à des dossiers pour lesquels (i) ils ne sont pas habilités et (ii) même s'ils sont habilités, ils ne doivent accéder qu'aux seuls dossiers strictement nécessaires à l'exécution de leur mission. En d'autres termes, l'Utilisateur doit limiter l'usage des accès dont il bénéficie exclusivement aux tâches professionnelles qui lui sont confiées et qui en nécessitent l'utilisation.

Si un mauvais comportement est observé, des investigations seront menées et les protagonistes seront entendus puis sanctionnés en cas d'accès illégitime avéré.

L'Utilisateur doit alerter son supérieur :

- S'il estime ne pas disposer des habilitations adaptées au bon exercice de ses activités professionnelles (qu'elles soient trop larges ou pas assez) ;
- S'il constate qu'une personne ne dispose pas des habilitations adaptées au bon exercice de ses activités professionnelles ;

Le supérieur s'assure que les droits d'accès accordés aux Utilisateurs sous sa responsabilité quittant leur service sont bien révoqués ou désactivés.

Enfin, en présence d'un traitement de Données personnelles (par exemple, l'utilisation de Données personnelles pour un projet de recherche, utilisation d'un nouvel outil IT impliquant des données personnelles), l'Utilisateur doit préalablement s'assurer qu'une revue de conformité a été effectuée (analyse d'impact, information des patients, contrat conforme, inscription au registre, formalité CNIL réalisée le cas échéant) par la DPO ou l'un de ses référents. Tout traitement de Données personnelles devra être effectué dans le respect des grands principes définis par le RGPD, rappelés dans la procédure interne dédiée à cet effet (limitation des finalités, minimisation des Données, confidentialité et sécurité, respect des droits des personnes).

Exemples de comportements abusifs et/ou sanctionnables :

- *Consulter tout ou partie du contenu du dossier médical d'un proche, d'une personnalité publique, d'un collègue, et d'une manière générale d'un patient en dehors de toute prise en charge de ce tiers. La consultation*

DRAFT

de son propre dossier n'est pas non plus autorisée (sauf si la personne concernée est son propre médecin traitant) ;
- *Consulter la paye d'un collègue ou son dossier disciplinaire en dehors d'une mission précise ;*
- *Révéler à des tiers non autorisés des informations couvertes par le secret ;*
- *Créer un dossier patient fictif ou utiliser le mode bris de glace de manière abusive ;*
- *Prendre des photos du dossier médical d'un patient.*
- *Diffuser l'image (photo / vidéo) d'un agent sans son autorisation explicite et préalable (l'image est une Donnée personnelle)*
- *Collecter et utiliser des Données de santé dans le cadre d'une recherche en dehors de tout cadre juridique ;*
- *Conserver dans son ordinateur des bases de Données personnelles sans encadrement sécurisé, ou mettre en production un projet impliquant un traitement de Données personnelles sans avoir consulté en amont la DPO.*

2.3. Accès privilégiés des Utilisateurs de la DSI

Certains Utilisateurs de la DSI disposent d'accès privilégiés à tout ou partie du SI et des applications métiers (y compris à celles traitant des Données personnelles), leur permettant de gérer et de contrôler leur bon fonctionnement et leur sécurité (ex. : maintenance et support aux Utilisateurs).

Par leurs fonctions mêmes, ces Utilisateurs peuvent avoir connaissance d'informations confidentielles protégées par la loi. En ce sens, les règles de confidentialité renforcées visées au précédent article s'appliquent à ces Utilisateurs, également soumis au secret professionnel.

Seuls les Utilisateurs habilités de la DSI sont autorisés à prendre la main à distance sur les Ressources des Utilisateurs, afin de résoudre les problèmes signalés. Durant les heures ouvrées, la prise de main devra être réalisée avec l'accord préalable de l'Utilisateur. Par exception, en cas de situation grave, et notamment en cas d'attaque virale, la prise de main à distance pourra être réalisée sur toutes les Ressources jugées suspectes sans requérir un accord préalable.

L'utilisateur s'engage à utiliser exclusivement à des fins professionnelles 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.

Exemples de comportements abusifs et/ou sanctionnables :
- *Utiliser ses droits d'accès privilégiés de manière abusive en dehors de tout cadre ou toute mission précise ;*
- *Faire preuve d'indiscrétion et révéler à des tiers des informations confidentielles ;*
- *Prendre connaissance des mots de passe ou des messages privés des Utilisateurs.*

3. Usage des Ressources

Synthèse :

- *Les Ressources sont mises à disposition des Utilisateurs à des fins professionnelles ;*
- *La configuration initiale des Ressources ne doit pas être modifiée pour des raisons de sécurité ;*
- *La connexion au SI de Ressources non fournies par l'AP-HP suppose l'accord préalable de la DSI ;*
- *Les informations professionnelles nécessaires à la continuité des activités doivent être sauvegardées sur les répertoires réseaux mis à disposition ;*
- *Les sessions des ordinateurs doivent être verrouillées dès que l'Utilisateur quitte son poste de travail ;*
- *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 obligations inhérentes au devoir de réserve, à la probité, à l'obligation de loyauté et au respect du secret professionnel s'appliquent en toutes circonstances.*

3.1. Usage professionnel et raisonné des Ressources

DRAFT

Les Ressources ont une finalité professionnelle et appartiennent à l'AP-HP. L'utilisation à titre personnel de certaines Ressources (précisément : téléphones fixes et portables, messagerie électronique, accès Internet) est tolérée de manière exceptionnelle et raisonnable.

L'Utilisateur doit veiller à clairement identifier la nature personnelle d'un message, d'un fichier ou d'une Donnée en indiquant « Privé » ou « Personnel » dans le titre de celui-ci ou en le stockant dans un répertoire portant cette même mention. L'Utilisateur fait seul son affaire personnelle et en temps utile de la sauvegarde et/ou de la destruction de ces messages et fichiers identifiés comme « personnels ».

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 fourni par l'AP-HP et non identifiés spécifiquement comme étant « personnels » seront, par défaut, considérés comme étant professionnels et pourront être utilisés et consultés par l'AP-HP pour assurer la continuité de l'activité.

Dans tous les cas, l'utilisation des Ressources :

- Doit être conforme aux lois et aux bonnes mœurs, et respecter les dispositions de la présente Charte et notamment les règles liées au secret médical ;
- Ne doit pas perturber ou porter préjudice à la sécurité du SI (risque d'encombrement ou d'engorgement du réseau) ;
- Ne doit pas nuire aux tâches professionnelles incombant à l'Utilisateur ou à l'image de l'AP-HP ;
- Ne doit pas porter atteinte aux règles de propriété intellectuelle qui interdisent notamment de télécharger, reproduire et/ou de diffuser des œuvres de l'esprit sans autorisation préalable de son propriétaire.

L'Utilisateur a une obligation générale et permanente de confidentialité et de discrétion attachée à l'utilisation des Informations, Données et documents électroniques disponibles sur le système d'information de l'AP-HP, et ce, pour la sauvegarde du patrimoine et des intérêts de celui-ci mais également des personnes concernées par ces informations, Données ou documents (patients, personnels, partenaires).

L'usage de la carte professionnelle CPS ou CPE est privilégié pour l'accès au SI.

Exemples de comportements abusifs et/ou sanctionnables :

- *Transformer des messages professionnels en « personnels » ;*
- *Introduire, exploiter ou tenter d'exploiter une faille de sécurité et/ou en faire la publicité ;*
- *Copier tout ou partie des codes sources d'un logiciel en dehors des droits autorisés par les licences correspondantes ;*
- *Tenir ou publier des propos dénigrants, diffamants, injurieux, homophobes ou sexistes (par téléphone, sur internet/intranet, par mail ou par tout autre moyen) ;*
- *Supprimer, altérer ou ne pas sauvegarder des informations nécessaires à la continuité de l'activité ;*
- *Subtiliser des documents professionnels.*

3.2. Utilisation du poste de travail

La configuration initiale du poste de travail doit être respectée car elle a été étudiée afin de garantir le bon fonctionnement et la sécurité du système d'Information. Elle ne doit jamais être modifiée sans l'accord préalable et écrit de la DSI. Les postes fixes ne doivent pas être déménagés d'un local à un autre sans autorisation.

Chaque Utilisateur doit :

- 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 ;
- Systématiquement verrouiller sa session s'il est amené à laisser la station de travail sans surveillance, et d'autant plus lorsque le poste est partagé entre plusieurs Utilisateurs.

Exemples de comportements abusifs et/ou sanctionnables :

DRAFT

- *Contourner ou désactiver les outils de sécurité, ou modifier leur paramétrage ;*
- *Télécharger ou utiliser des logiciels métiers non autorisés par la DSI ;*
- *Laisser son ordinateur sans surveillance et/ou sans code.*

3.3. Utilisation de la messagerie professionnelle

La messagerie est professionnelle et appartient à l'AP-HP. L'Utilisateur est responsable du contenu et de la forme de tout message qu'il émet avec son adresse de messagerie AP-HP :

- Tout message envoyé depuis l'adresse professionnelle AP-HP, associe 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 ;
- L'Utilisateur doit faire preuve de politesse et de la plus grande correction à l'égard de ses interlocuteurs lors des échanges ;
- L'Utilisateur doit faire preuve de vigilance vis-à-vis de l'identité des auteurs des messages reçus, notamment de correspondants extérieurs. En effet, la falsification de l'identité de l'auteur d'un message est facilement réalisable sur Internet
- L'Utilisateur veille à ne pas ouvrir les messages et les pièces jointes qui semblent avoir une origine inconnue ou douteuse ; il est recommandé de consulter le supérieur hiérarchique en cas de doute ;
- Chaque Utilisateur est responsable de la confidentialité attachée aux messages. L'utilisation d'une messagerie sécurisée certifiée (ex. MS Santé) est obligatoire pour tout échange de Données personnelles relatives à la santé avec d'autres professionnels de santé en dehors de l'AP-HP ; pour les échanges de Données personnelles de santé avec un patient, le professionnel de santé doit obtenir son consentement préalable éclairé ;
- Les échanges de Données personnelles relatives à la santé peuvent également être réalisés via des outils sécurisés validés par la DSI (Ex. : Dispose), à condition d'être supprimées immédiatement une fois l'échange réalisé).

En cas de réception à tort d'un message destiné à une autre personne, l'Utilisateur doit le renvoyer à son expéditeur en indiquant l'erreur d'adressage et doit le supprimer définitivement de sa messagerie.

S'agissant spécifiquement de l'utilisation de la messagerie à des fins syndicales, ceci est autorisé à condition de respecter la législation en vigueur, les accords collectifs applicables à l'AP-HP et de respecter les principes posés dans la présente Charte. L'utilisation de la messagerie électronique à des fins syndicales doit être compatible avec les exigences de bon fonctionnement du système d'information et ne pas entraver l'accomplissement du travail confié à l'Utilisateur.

Exemples de comportements abusifs et/ou sanctionnables :

- *Utiliser les listes de diffusion à des fins inappropriées ;*
- *Utilisation malveillante de la mention « Privé » ou « Personnel » sur des messages pourtant professionnels ;*
- *Utilisation abusive de la messagerie syndicale ;*
- *Activer le reroutage automatique et permanent de ses messages vers une adresse tierce à l'AP-HP non sécurisée, sans justification précise et alors qu'un moyen alternatif sécurisé existe ;*
- *Utiliser une messagerie non sécurisée (de type Gmail ou Whats app) pour échanger des données de santé ;*
- *Mettre à disposition d'autrui des informations sensibles sans y être préalablement autorisé ;*
- *Détourner ou utiliser des informations afin d'émettre de fausses déclarations, falsifier les Données , supprimer ou modifier des Données au préjudice de l'AP-HP ;*
- *Intercepter des documents classifiés confidentiels, par un quelconque stratagème frauduleux ;*
- *Envoyer des messages en masse sans lien avec l'activité professionnelle.*

3.4. Utilisation d'internet et d'intranet

Internet :
Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle de l'Utilisateur. L'accès à des sites Internet initialement bloqués par l'AP-HP est interdit sauf cas dérogatoire. 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 interdit, avec un équipement fourni par l'AP-HP, d'utiliser des réseaux WIFI externes dans les locaux de l'AP-HP pour accéder à Internet.

A titre exceptionnel, dans la limite d'une utilisation raisonnable, l'utilisation d'un WiFi hors réseau AP-HP, fourni par certains services (ex. : SAMU), est tolérée lors des temps de pause, exclusivement avec des équipements personnels (ordinateur portable, tablette…). Il est interdit de connecter des équipements du SI de l'AP-HP à ces réseaux qui ne sont, par définition, pas sécurisés. Il est également interdit d'installer ou d'utiliser une borne privée Wifi sans autorisation préalable.

L'AP-HP peut bloquer l'accès à tout site Internet non indispensable aux activités professionnelles ou présentant un risque d'incident de sécurité. Par ailleurs, les sites dont le contenu peut être contraire à l'ordre public ou aux bonnes mœurs (par exemple, site contenant des éléments pornographiques, indécents, incitants à la haine ou relatifs au piratage informatique) sont interdits à la consultation et en principe bloqués par les règles de filtrage.

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 professionnels ou pas, 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 dans la présente charte, sans porter atteinte à l'image de marque de l'AP-HP et dans le respect des codes de déontologie professionnelle pour les professions qui en disposent.

Chaque Utilisateur doit se conformer aux restrictions d'utilisation (respect de la propriété intellectuelle) des logiciels fournis par l'AP-HP. Enfin les Utilisateurs doivent être vigilants quant à l'utilisation de logiciel de visioconférence non sécurisée et s'adresser à leur supérieur hiérarchique avant de télécharger ces outils tiers. De manière générale aucun outils tiers ne doit être installé sur le SI de l'AP-HP sans autorisation préalable de la DSI.

Intranet :
L'Intranet est mis à la disposition de certains Utilisateurs à des fins exclusivement professionnelles. L'Intranet doit être utilisé de manière rationnelle, loyale et responsable. L'Intranet est destiné à promouvoir la communication, à faciliter l'interaction sociale entre les Utilisateurs et à améliorer l'efficacité et la qualité du travail de chacun. En fonction du poste occupé, de la fonction, du statut, ou encore du rang hiérarchique, un Utilisateur peut être habilité à accéder à certaines Informations, applications, fonctionnalités ou contenus spécifiques. Tout Utilisateur est responsable de l'usage de l'Intranet auquel il a accès et reste seul responsable des Informations qu'il publie ou échange sur l'Intranet.
L'Utilisateur veillera enfin a respecter les droits de propriété intellectuelle des auteurs des publications effectuées sur l'Intranet.

Exemples de comportements abusifs et/ou sanctionnables :

- *Utiliser des réseaux wifi publics non sécurisés alors que le partage de connexion avec le téléphone professionnel est possible ;*
- *Utiliser Internet à des fins commerciales ou ludiques ou contraires aux bonnes mœurs (ex : Alimenter un blog, télécharger des films) ;*
- *Porter atteinte à la vie privée des personnes en publiant des informations ciblées relatif à la santé, à la vie sexuelle ou encore aux opinions religieuses d'un tiers ;*
- *Nuire à l'image de marque de l'AP-HP, à ses intérêts ou à sa réputation, de quelque manière que ce soit;*
- *Ne pas respecter les droits de propriété intellectuelle des tiers lors de la publication d'information sur l'intranet / l'internet.*

3.5. Utilisation du téléphone

Les téléphones portables et les smartphones permettant de stocker et/ou d'accéder aux informations parfois confidentielles de l'AP-HP, doivent être protégés. 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 »).

Exemples de comportements abusifs et/ou sanctionnables :

- *Ne pas mettre de code de sécurité sur son portable, ou choisir un code facilement identifiable ;*
- *Appeler des numéros surtaxés ou appeler l'étranger quand ce n'est pas strictement nécessaire à l'activité professionnelle ;*
- *Utiliser son téléphone professionnel à des fins personnelles de manière excessive.*

3.6. Utilisation des espaces de stockage

Les informations professionnelles nécessaires à la continuité des activités doivent être sauvegardées sur les espaces de stockage et répertoires réseaux mis à disposition des Utilisateurs.

- Les Utilisateurs sont responsables des informations qu'ils stockent sur ces Ressources ;
- Les documents et les messages professionnels doivent être systématiquement archivés, notamment ceux 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 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 ou confidentielles, 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 ;
- L'Utilisateur doit veiller à supprimer en temps utile les éventuels fichiers de Données personnelles conservés sur les espaces de stockage, dès lors qu'il n'a plus besoin de les conserver pour les besoins de sa mission.

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.

Exemples de comportements abusifs et/ou sanctionnables :

- *Supprimer des éléments nécessaires à la continuité de l'activité ;*
- *Conserver de manière illimitée des fichiers de données personnelles ;*
- *Ne pas sauvegarder systématiquement les informations professionnelles ;*
- *Stocker des données contraire à la loi ou aux bonnes mœurs ;*
- *Stocker des Données personnelles en clair dans des espaces de stockage non sécurisés.*

3.7. Utilisation des supports amovibles et imprimantes

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

Les supports amovibles, tels que les clés USB, 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.

Des supports amovibles sécurisés peuvent être ainsi délivrés aux Utilisateurs qui en ont besoin. 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 DSI de son Groupe Hospitalier ou de son site, qui pourra lui indiquer comment procéder à son analyse.

Les imprimantes sont souvent partagées, de ce fait, tout document confidentiel (ex. : contenant des Données à personnelles relatives aux patients ou aux agents) doit être récupéré rapidement.

Exemples de comportements abusifs et/ou sanctionnables :

DRAFT

- *Laisser des documents confidentiels ou contenant des Données sensibles aux imprimantes ;*
- *Stocker des données sensibles (des patients ou agents de l'AP-HP) en clair sur une clé USB non sécurisée ;*
- *Ne pas sauvegarder les informations stockées uniquement sur une clé USB.*

3.8. Utilisation de Ressources personnelles

Les règles applicables dans la présente Charte s'appliquent également aux Ressources non fournies par l'AP-HP et interagissant avec le SI de l'AP-HP (équipement personnel ou fourni par des tiers). Chaque Utilisateur doit veiller à ne pas connecter des ressources personnelles dont l'origine est suspecte.

Pour des raisons de sécurité, la connexion au système d'information de l'AP-HP, sur site ou à distance, de tout équipement ou matériel personnel non sécurisé (notamment ordinateurs, téléphones, tablettes, clé USB) est interdite sans autorisation de la DSI et/ou paramétrage préalable par la DSI (ex. installation de Citrix). Il est précisé que l'accès à distance avec un ordinateur personnel via le réseau wifi sécurisé de l'AP-HP ou via un lien sécurisé (VPN fourni par la DSI) permettant d'accéder aux applications est autorisé.

Il est demandé à chaque Utilisateur de privilégier l'usage de matériels sécurisés fournis par l'AP-HP, et de ne les connecter qu'à des postes de travail sécurisés (pourvus d'un antivirus).

L'Utilisateur d'un équipement personnel mobile doit prendre des précautions supplémentaires pour éviter le vol de cet équipement et la perte des données qui y sont stockées. Les données professionnelles stockées sur un équipement personnel mobile doivent être régulièrement sauvegardées sur le réseau de l'AP-HP. Il est interdit de stocker des fichiers de Données personnelles sur des équipements personnels.

En cas de doute, l'Utilisateur s'adressera à son supérieur hiérarchique afin de mettre en œuvre les mesures de protection pour préserver la sécurité et la confidentialité des informations stockées.

Exemples de comportements abusifs et/ou sanctionnables :

- *Utiliser des clés USB non fiables ou dont la provenance est incertaine ou douteuse (ex. Goodies) ;*
- *Laisser un équipement personnel sans surveillance ;*
- *Ne pas installer ou désactiver les outils de sécurité sur son équipement personnel.*

4. Traçabilité, contrôle et audits

Synthèse :

- *Toutes les actions des Utilisateurs sur le SI de l'AP-HP sont tracées ;*
- *Des audits ciblés et aléatoires sont menés périodiquement afin de contrôler les accès et usages des Ressources, particulièrement s'agissant des accès aux dossiers patients informatisés ;*
- *En cas d'accès illégitime avéré et après convocation de l'Utilisateur fautif, des sanctions sont appliquées.*

4.1. Traçabilité et contrôle

Des mesures de contrôle et de suivi sont mises en œuvre dans le strict respect des principes de transparence et de proportionnalité des moyens de collecte, ceci uniquement à des fins de sécurité, de protection et de vérification du bon accès et usage des Ressources dans le respect des règles éditées par la présente charte et pour assurer la continuité de l'activité.

Les services compétents de l'AP-HP tracent quotidiennement les actions des Utilisateurs afin de :

- De contrôler le respect du secret professionnel à travers les contrôles de traces portant sur les outils métiers, particulièrement s'agissant de l'accès aux dossiers médicaux informatisés ;

DRAFT

- De garantir le bon fonctionnement des Ressources, le volume d'utilisation, de détecter des anomalies de faire évoluer les Ressources en fonction des besoins ;
- De vérifier que les règles en matière de sécurité sont correctement appliquées et conformes à la politique de sécurité ;
- De détecter toute défaillance ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ;
- De contrôler plus généralement le respect des règles d'utilisation et de sécurité du système d'information ;
- De pouvoir identifier et, le cas échéant, sanctionner des usages contraires à la présente charte, aux législations et réglementations applicables ;
- De pouvoir fournir des preuves nécessaires pour mener les enquêtes en cas de contentieux visant un Utilisateur ou un tiers, ou plus généralement de répondre aux requêtes des autorités publiques habilitées (services de police, autorités judiciaires…).

Précisément, l'AP-HP surveille, analyse et audit de façon périodique les dispositifs professionnels dont :
- L'utilisation d'ORBIS ou autres dossiers patients informatisés, mais également HR Access
- 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.

Cette surveillance consiste en une analyse des traces laissées par l'Utilisateur à l'occasion de l'utilisation des Ressources. 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 consultées, 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).

Les traces de connexion au système d'information sont conservées pendant 1 an (sauf obligations légales ou réglementaires particulières de conserver ces données sur une durée plus longue), puis archivées de manières anonymes pendant 2 ans à des fins statistiques (nombre de messages émis vers ou reçus de l'Internet, volumes occupés par l'ensemble des boîtes aux lettres, sites Internet les plus visités, fréquence d'accès à l'internet ou à l'Intranet, nombre de pages visitées, nature des pages visitées, date heure et durée de connexion, taille des espaces sur les serveurs de fichiers, durées totales des connexions distantes, etc.). Les Utilisateurs sont précisément informés des conditions de traitement des données personnelles sur l'intranet de l'AP-HP.

4.2. Accès par l'AP-HP aux Ressources de l'Utilisateur

Pour assurer la continuité de son activité ou en cas de risque (par exemple, risque de sécurité, d'atteinte à la confidentialité ou de non-conformité réglementaire), l'AP-HP pourra accéder et consulter :
- Les traces nominatives d'un Utilisateur aux applications ;
- L'ensemble des Données, messages et fichiers professionnels stockés dans les Ressources confiées à l'Utilisateur. Dans ce cas et si les Données, messages et fichiers ont une nature personnelle, l'AP-HP pourra y accéder en présence du propriétaire ou celui-ci dûment prévenu.

Les modalités d'accès 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 après avoir été préalablement informé, et à défaut de la présence du professionnel de santé, celle d'un représentant de la Commission Médicale d'Etablissement Locale ou Centrale.

DRAFT

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.

Il est précisé que l'accord / la présence des différents Utilisateurs ci-dessus n'est pas requise en cas d'urgence (ex. : risque de sécurité du SI ou manquement réglementaire) ni pour les audits des traces nominatives d'un Utilisateur aux applications.

4.3. Audits réalisés afin de prévenir et sanctionner les accès illégitimes (violation du secret)

Dans l'objectif de prévenir et sanctionner les accès illégitimes aux dossiers traitant des Données personnelles ou dans l'EDS, l'Utilisateur est informé que des audits sont menés par la DSI, visant à étudier les traces d'accès aux dossiers traitant des Données personnelles.

Deux types d'audits peuvent être entrepris :

- Des audits ciblés sur un ou plusieurs Utilisateurs, en cas de signalement remonté à la DPO, par un tiers ou par la personne concernée (demande de droit d'accès suite à une suspicion d'accès illégitime au dossier médical) ;
- Des audits aléatoires sur un ou plusieurs Utilisateurs choisis au hasard, sur une journée donnée.

La procédure d'audit est en synthèse la suivante :

- Recherches des traces d'accès aux données de santé par les Utilisateurs habilités de la DSI ;
- Présentation des analyses pseudonymisées en commission dédiée à cet effet (la 3CADP, en charge de donner un avis sur la pré qualification de la licéité ou pas des accès) ;
- Édition du rapport de contrôle, co-signé par la DPO et le DIM central ;
- Convocation des agents incriminés par la hiérarchie (ex. : DRH locale, le chef de service, le directeur de DMU et/ou le président de la CME, (selon la fonction de l'Utilisateur) pour confirmer ou infirmier le caractère illégitime des accès;
- Sanctions en cas d'accès illégitime avéré.

4.4. Remontée des incidents

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
- Au responsable hiérarchique ou
- Sur la plateforme dédiée à cet effet (Osiris).

En outre, en cas d'accès accidentel à un mail, une pièce jointe ou un site Internet illicite ou potentiellement dangereux (site corrompu ou susceptible d'être vecteur d'une infection virale), l'Utilisateur doit immédiatement se déconnecter et informer le support SI.

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

5. Sanctions

DRAFT

En cas de non-respect de la présente charte, l'AP-HP se réserve le droit de prendre des sanctions disciplinaires, dans le respect des procédures applicables, et ceci sans préjuger des éventuelles poursuites judiciaires, pénales et ordinales qui pourraient être initiées à l'encontre des Utilisateurs concernés.

A titre d'exemples :

- Au titre des sanctions disciplinaires, l'Utilisateur fautif encourt :
    - Un avertissement
    - Un blâme
    - Une radiation du tableau d'avancement ou une rétrogradation au grade inférieur
    - Une exclusion temporaire ou définitive
    - Un licenciement ou révocation

- Au titre des sanctions pénales :

    - L'Utilisateur soumis au secret peut être condamné à un an d'emprisonnement et 15 000 euros d'amende en cas de révélation d'une information à caractère secret ;

    - L'Utilisateur qui accède frauduleusement dans un SI 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.

- Au titre des sanctions ordinales, l'Utilisateur fautif peut être condamné par ses pairs et encourir une interdiction temporaire ou définitive d'exercer (radiation).

Les sanctions seront appliquées proportionnellement à la gravité de la faute commise et au préjudice subi.

Nonobstant les sanctions visées ci-dessous, l'AP-HP pourra également procéder à la restriction ou à la suspension immédiate des droits d'accès de l'Utilisateur à tout ou partie des Ressources informatiques. L'Utilisateur est alors informé par écrit des constats motivant l'intervention et pourra faire valoir sa position.

L'AP-HP pourra également décider une suspension immédiate des droits d'accès à titre conservatoire.

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 la Charte pourra engendrer la rupture dudit contrat sans préjudice de tout dommages et intérêts que l'APHP pourrait être fondée à réclamer.

6. Entrée en vigueur et procédure

La présente Charte entre en vigueur à compter de sa date de publication sur l'intranet de l'AP-HP. Une communication spécifique est réalisée à cet effet sur (…).

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 après :

- Information de la commission centrale et des commissions locales des soins infirmiers, de rééducation et médicotechniques, en date du (…)
- Information des doyens des UFR de médecine de la Région Ile de France en date du (…)
- 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 en date du (…)
    - Le comité technique d'établissement central, lors de la séance en date du (…);
- Consultation de la commission médicale d'établissement, lors des séances en date du (…);
- Soumission pour avis au conseil de surveillance lors de la séance en date du (…);

DRAFT

- Soumission pour avis au Directoire lors de la séance en date du (…);

La Charte sera modifiée en fonction du contexte législatif et réglementaire. Toute modification 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, la DPO, le Responsable Sécurité du Système d'Information de votre entité ou de l'AP-HP peuvent être consultés.

7. Annexes

DRAFT

Annexe 1 : Définitions

3CADP : désigne la Commission Centrale de Contrôle des Accès aux Dossiers Patients associant notamment la DPO, le DIM central et la DAJDP, dont la mission est de préqualifier le caractère illégitime des accès aux outils traitant des Données personnelles

CME : désigne la Commission médicale d'établissement

CNIL : désigne la Commission Nationale Informatique et Libertés, créée par la loi Informatique et Libertés du 6 janvier 1978 et chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, publics et privés. La CNIL a un pouvoir de contrôle et de sanction.

Données personnelles : désigne toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (exemple : un nom, une photo, une radio, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc.)

Données personnelles sensibles : désigne des Données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des Données génétiques, des Données biométriques aux fins d'identifier une personne physique de manière unique, des Données concernant la santé ou des Données concernant la vie sexuelle.

Données personnelles de santé : désigne les Données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

DAJDP : désigne la Direction des Affaires juridiques et des Droits des Patients de l'AP-HP

DIM : désigne le Département de l'Information Médicale

DMU : désigne les Départements Médicaux Universitaires

DPO : désigne le délégué à la protection des données de l'AP-HP désigné à la CNIL, en charge de contrôler la conformité de l'AP-HP au regard de la réglementation applicable en matière de protection des données personnelles

DRH : désigne la Direction des Ressources Humaines

DSI : désigne la Direction des Systèmes d'information de l'AP-HP

EDS : désigne l'Entrepôt de Données de santé de l'AP-HP

LIL : désigne la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Ressources informatiques ou Ressources : désigne tout élément physique ou logique, matériel, informatique, interagissant avec tout ou partie du SI de l'AP-HP et comprenant :

- Des éléments matériels, tels que notamment : infrastructures de tout type, serveurs, data center, mais également les hubs, firewalls, équipements réseaux, équipements individuels remis à l'Utilisateur, tout périphérique et tout autre matériel informatique, connectique ou bureautique en ce compris les plateformes, câbles du réseau, photocopieurs, ordinateur et téléphones fixes ou portables, scanners, imprimantes, etc.;

DRAFT

- Des éléments logiciels ou immatériels tels que notamment le système d'information (SI), les réseaux, les logiciels, progiciels, applications, fichiers, Données et bases de Données, l'intranet, l'extranet, le système de messagerie, les services Internet, etc.
- Les règles applicables dans la présente Charte s'appliquent également aux Ressources non fournies par l'APHP et interagissant avec le SI de l'APHP (équipement personnel ou fourni par des tiers).

RGPD : désigne le Règlement Général sur la Protection des Données personnelles (RGPD), qui fixe le cadre légal en matière de protection des données personnelles

RSSI : désigne le responsable de la sécurité des système d'information de l'AP-HP

Secret médical : désigne l'obligation de discrétion professionnelle imposée à l'ensemble du personnel de l'AP-HP, et représente un droit fondamental pour le patient. La violation du secret médical, (condamnable par le code pénal et le code de la santé publique) est par exemple caractérisée lorsque des tiers non autorisés accèdent, quand bien même ils auraient les habilitations pour le faire, aux Données de santé de patients à l'insu de ces derniers et en dehors du cadre de la prise en charge.

Secret professionnel : désigne le principe de confidentialité applicable à certaines fonctions (Ressources humaine, DSI) qui implique l'interdiction de divulguer à des tiers ou à des personnes non autorisées, des informations à caractère confidentiel (information sur les salaires notamment).

SI : désigne le Système d'information de l'AP-HP

Utilisateur : désigne :

- Toute personne physique membre du personnel de l'AP-HP, quel que soit son statut (professionnel de santé ou pas), son niveau hiérarchique ou son lieu d'accès, notamment : les salariés, les fonctionnaires, les contractuels, les apprentis, les stagiaires, ou encore les intérimaires qui, de manière permanente ou occasionnelle accède et/ou utilise les Ressources de l'AP-HP ;
- Toute personne physique non membre du personnel de l'APHP, tel que les enseignants, les étudiants, chercheurs, mais également les prestataires externes ou les sous-traitants, qui accèdent à tout ou partie du SI de l'AP-HP. Les Utilisateurs de l'APHP chargés des relations contractuelles et opérationnelles avec ces tiers doivent s'assurer (i) de la communication de cette Charte à ces tiers avant la signature du contrat et (ii) du respect de ses règles par ces tiers.

Violation de Données personnelles : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données.

Annexe 2 : Référentiel légal

Dans le cadre de l'accès et de l'utilisation des Ressources, les Utilisateurs se doivent d'être en conformité vis-à-vis des lois et des réglementations en vigueur, en particulier :

- Le Code Pénal :
  - Atteinte au secret médical
  - Consultation illégitime d'un dossier patient en dehors de la prise en charge
  - Intrusion frauduleuse dans un SI, fraude informatique
  - Usurpation d'identité
  - Atteinte aux bonnes mœurs (diffamation, injure, incitation à la haine, pornographie...)

- Le Code de la Santé Publique :
  - Respect absolu du secret médical, de la déontologie et des règles éthiques associées
  - Respect des règles d'accès aux dossiers patients

  - Respect des conditions d'hébergement de Données de santé

- Le Règlement Général sur la Protection des Données personnelles (RGPD) et la Loi Informatique, Fichiers et Libertés (LIL) :
  - Revues de conformité / analyses d'impacts / inscription au registre
  - Information des personnes et collecte de Données strictement nécessaire à la finalité
  - Respect des droits des personnes (opposition, rectification, etc…)

- Le Code civil :
  - Secret des correspondances
  - Respect de la vie privée
  - Respect du droit à l'image

- Le Code de la Propriété Intellectuelle :
  - Protection des logiciels, des écrits, des images, des marques et des bases de Données, des publications des recherches (contrefaçon)
  - Téléchargement illégaux
  - Respect des autorisations accordées

- Le Code du travail :
  - Application des sanctions disciplinaires
  - Procédures de sanctions (convocation, échelle des sanctions)

- Les codes de déontologie applicables aux Utilisateurs :
  - Respect absolu du secret médical, de la déontologie et des règles éthiques associées
  - Respect des règles d'accès aux dossiers patients

- Les procédures internes applicables au sein de l'AP-HP et les documentations d'information notamment disponible sur l'intranet et les réseaux partagés internes.

DRAFT