

Sécurité dans la relation avec les Fournisseurs

DSN/SSI

Version 1.1

Table des matières

1	OBJECTIFS.....	3
2	PERIMETRE D'APPLICATION	3
3	DESCRIPTION	4
3.1	SECURITE DE L'INFORMATION DANS LES RELATIONS AVEC LES FOURNISSEURS	4
3.2	SURVEILLANCE, AUDIT ET REVUE DES FOURNISSEURS.....	4
4	EXIGENCES DE SECURITE	7
4.1	PROTECTION DES DONNEES PERSONNELLES	7
4.2	CONFIDENTIALITE	8
4.3	SECURITE.....	9
4.4	LES EXIGENCES FONCTIONNELLES DE SECURITE	13
4.5	METHODOLOGIE SECURISEE D'INGENIERIE ET DE DEVELOPPEMENT.....	15
4.6	AUDITS	16
5	ANNEXES	18
	DEFINITIONS	18
	CHECKLIST	18
	COORDONNEES.....	19
	MATRICE IMPACT-GRAVITE.....	20

I OBJECTIFS

Les objectifs de ce document sont de :

- Garantir la protection des actifs de l'AP-HP accessibles aux Fournisseurs
- Maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux Marchés conclus avec les Fournisseurs

Le document décrit les exigences générales minimales de sécurité en réponse à ces objectifs et les modalités de surveillance, d'audit et de revue des Fournisseurs.

2 PÉRIMÈTRE D'APPLICATION

Ce document s'applique à tout le SI de l'APHP.

QUOI			
Système d'Information Essentiel	SI Hébergeur de Données de Santé	SI Biomédicaux et Techniques	Autres SI
✓	✓	✓	✓

QUI				
Patients Usagers	Personnels AP-HP	Professionnels tiers	Étudiants	Fournisseurs
		✓		✓

3 DESCRIPTION

3.1 Sécurité de l'information dans les relations avec les Fournisseurs

L'AP-HP joint aux Marchés avec les Fournisseurs les exigences minimales de sécurité de l'information auxquelles les Fournisseurs doivent se conformer pour limiter les risques résultant de l'accès des Fournisseurs aux actifs ou de la fourniture de composants de l'infrastructure informatique de l'AP-HP.

L'[Article 5](#) « Confidentialité - Protection des données personnelles - Mesures de sécurité » du cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication (CCAG TIC) (NOR : ECOM2106875A) est applicable pour les marchés relevant du CCAG TIC.

L'[Article 5](#) « Confidentialité - Protection des données personnelles - Mesures de sécurité » du cahier des clauses administratives générales des marchés publics de techniques de l'information et de la communication (CCAG FCS) (NOR : ECOM2106868A) est applicable pour les marchés relevant du CCAG FCS.

L'Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité (NOR : ECOP1825228A) est applicable.

Le présent document complète et précise les dispositions de l'Article 5 du CCAG TIC et du CCAG FCS ainsi que l'arrêté 18 septembre 2018.

La présente procédure comporte une checklist permettant à l'AP-HP de préciser de manière synthétique le contexte d'intervention du Fournisseur. Cette checklist facilite l'identification par le Fournisseur de ses obligations (Cf. annexe).

Le Fournisseur identifie un point de contact administratif au sein de son organisation qui sera destinataire des notifications de violation de données personnelles pour les personnes concernées qui relèveraient de la responsabilité du Fournisseur.

Le Fournisseur identifie un point de contact technique au sein de son organisation qui sera chargé de gérer les accès aux locaux et aux systèmes d'information de l'AP-HP pour le compte du Fournisseur.

Le processus de gestion des relations avec les Fournisseurs est mis en œuvre par le Pôle d'Intérêt Commun (PIC) AGEPS de l'AP-HP en collaboration avec la Direction des Services Numériques (DSN).

Pour les services, le Fournisseur a l'obligation de diffuser la documentation spécifique à la sécurité de l'information de l'AP-HP jusqu'au dernier maillon de la chaîne d'approvisionnement si le Fournisseur sous-traite des parties des services rendus à l'AP-HP.

Pour les produits informatiques, le Fournisseur a l'obligation de diffuser les pratiques de sécurité appropriées jusqu'au dernier maillon de la chaîne d'approvisionnement si ces produits comportent des composants achetés chez d'autres Fournisseurs.

3.2 Surveillance, Audit et Revue des Fournisseurs

L'AP-HP surveille, revoit et audite à intervalles réguliers les prestations de service assurées par les Fournisseurs afin de s'assurer que les exigences de sécurité de l'information prévues dans les Marchés sont bien respectées et que les incidents et les problèmes liés à la sécurité de l'information sont gérés correctement.

Les Fournisseurs ont pour obligation de constituer les preuves de conformité aux exigences de sécurité. L'AP-HP demande la communication de ces preuves dans le cadre de la présente procédure.

Le degré de surveillance des Fournisseurs dépend des critères suivants :

- La criticité métier des projets ou des actifs sur lesquels le Fournisseur intervient
- Le degré d'interconnexion du Fournisseur avec le système d'information de l'AP-HP
- L'accès du Fournisseur à des données sensibles ou confidentielles
- L'exposition du service fourni sur Internet
- Les rapports de surveillance précédant
- Les incidents de sécurité passés.

Le programme de revue est élaboré sur la base de ces critères par le pôle sécurité de la DSN et soumis à validation à la Déléguée à la protection des données, à l'AGEPS et au Directeur de la DSN ou son représentant.

Pour la première année de mise en œuvre de la présente procédure, seuls 3 Fournisseurs font l'objet d'une revue. Un bilan sera effectué afin d'adapter si besoin la présente procédure.

La revue fait l'objet d'un entretien formel en présence du Fournisseur et d'un ou plusieurs représentants de l'AP-HP.

La revue comprend :

1. La surveillance des niveaux de performance des prestations et la vérification de leur conformité avec les Marchés
2. Les comptes-rendus des réunions régulières de suivi des prestations
3. Les changements significatifs (Marchés, organisation, prestations)
4. Les problèmes d'exploitation, les défaillances et le suivi des pannes et des interruptions liées au service fourni
5. Les rapports relatifs aux incidents liés à la sécurité de l'information ainsi que les retours d'expérience incluant la description des actions correctives et curatives avec leur état d'avancement
6. La sécurité de l'information dans les relations du Fournisseur avec ses propres sous-traitants
7. Les rapports d'audit par l'AP-HP sur la période écoulée
8. L'évolution de la capacité du Fournisseur à maintenir un niveau de continuité de service convenu en cas de défaillance majeure du service ou de sinistre.

Répartition des Rôles dans la gestion des relations avec les Fournisseurs :

- L'AGEPS est responsable de la gestion des relations avec les Fournisseurs sur le plan juridique et administratif y compris les mises en demeure en cas de manquements
- La Déléguée à la protection des données apporte son expertise en matière de protection des données personnelles. Elle contribue à la procédure de revue des fournisseurs
- Le pôle SSI de la DSN apporte son expertise en matière de sécurité de l'information. Il tient à jour le registre des fournisseurs les plus critiques. Il propose annuellement le programme de revue des fournisseurs
- Le pôle Ressources de la DSN assure l'exécution du marché.
- Le pôle de la DSN, qui assure le volume prestation le plus élevé avec un Fournisseur, est désigné comme chef de file. Il est chargé d'organiser et de conduire la revue avec le Fournisseur dans les locaux de l'AP-HP ou à défaut à distance. Il saisit l'AGEPS lorsque des insuffisances sont observées dans les prestations en informant les pôles Ressources et Sécurité de la DSN et la Déléguée à la protection des données
- Le Fournisseur constitue le fonds documentaire nécessaire à la revue. Il le communique au pôle chef de fil 7 jours calendaire avant la tenue de la revue. Le Fournisseur produit le compte-rendu de la revue sous 2 jours ouvrés. L'AP-HP dispose de 7 jours pour émettre ses observations et valider le compte-rendu dès qu'il n'y a plus d'observations.

Pour les autres Fournisseurs, une revue est organisée à la fin du Marché ou en cas de changement important dans le volume ou la nature des prestations, de rachat, de changement de pays...

En cas de survenance d'un incident de sécurité d'une gravité supérieure ou égale à 3 (Cf. Matrice Impact-Gravité à la page n°20) ou lors de l'identification d'un risque critique impliquant le Fournisseur, un audit de sécurité du Fournisseur pourra être diligenté par l'AP-HP.

4 EXIGENCES DE SÉCURITÉ

4.I Protection des données personnelles

Dans le cadre de leurs relations contractuelles, le Fournisseur et l'AP-HP s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 en vigueur (ci-après, « le règlement européen sur la protection des données »), la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée et le Code de la Santé Publique (CSP).

4.1.1 Traitements réalisés par l'AP-HP

Dans le cadre de son activité, l'AP-HP collecte des données à caractère personnel du Fournisseur, qui font l'objet de traitements automatisés dans les conditions prévues par la loi n°78-17 précitée, à des fins (a) de gestion de la relation Fournisseur (facturation, assistance et maintenance des Services, gestion commerciale, archivage, téléphonie, amélioration de la qualité, de la sécurité et de la performance des services, recouvrement, etc.), et (b) de respect de la réglementation applicable à l'AP-HP (notamment obligations légales de conservation des données de connexion et d'identification des utilisateurs).

L'AP-HP s'engage à ne pas utiliser les données ainsi collectées à d'autres fins que celles susmentionnées. L'AP-HP peut toutefois être amenée à devoir les communiquer à des autorités judiciaires et / ou administratives, notamment dans le cadre de réquisitions. En ce cas, et sauf disposition légale l'en empêchant, l'AP-HP s'engage à en informer le Fournisseur et à limiter la communication de données à celles expressément requises par lesdites autorités.

Les données traitées à des fins de gestion de la relation entre le Fournisseur et l'AP-HP sont constituées d'informations telles que NOM, prénom, adresse postale, adresse électronique, numéro téléphone et sont conservées par l'AP-HP pendant toute la durée du Marché et les trente-six (36) mois suivants. Les données de connexion et d'identification sont conservées par l'AP-HP pendant douze (12) mois. Les autres données à caractère personnel collectées et traitées par l'AP-HP afin de respecter ses obligations légales, sont conservées conformément à la loi applicable.

Dans le cadre des finalités définies ci-dessus, le Fournisseur accepte que les données à caractère personnel susvisées le concernant soient transférées par l'AP-HP à ses sous-traitants qui interviennent dans le cadre de l'exécution des Marchés. Celles-ci ne pourront toutefois accéder à ces données à caractère personnel que dans le cadre des finalités susmentionnées, et dans le strict respect des droits du Fournisseur en matière de protection des données à caractère personnel.

Conformément à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée, le Fournisseur bénéficie d'un droit d'accès, de rectification et de suppression des informations susvisées le concernant. Il peut exercer ce droit et obtenir communication desdites informations auprès du Délégué à la Protection des Données (DPO) de l'AP-HP (Cf. coordonnées en annexe) en justifiant de son identité. Il y sera répondu dans un délai de trente (30) jours suivant réception.

Le Fournisseur dispose également du droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

4.2 Confidentialité

Le Fournisseur qui, soit avant la notification du Marché, soit au cours de son exécution, a reçu communication, à titre confidentiel, de renseignements ou de documents quelconques, est tenu de maintenir confidentielle cette communication.

L'obligation de confidentialité s'étend aux données intéressant les patients et les personnels de l'AP-HP dont le Fournisseur, pourrait avoir connaissance dans le cadre de l'exécution des prestations.

Dans tous les cas, ces renseignements ou documents ne peuvent pas, sans autorisation, être communiqués à d'autres personnes que celles qui ont qualité pour les connaître.

Le Fournisseur se porte fort du respect par ses salariés et sous-traitants et plus généralement de toutes personnes – personnes morales comme personnes physiques - intervenant pour le compte du Fournisseur du principe de confidentialité des données précitées.

Indépendamment de l'éventuel engagement de sa responsabilité pénale, il assumera donc à ce titre, à l'égard de l'AP-HP, toutes conséquences de droit, en cas de divulgation des informations confidentielles par ses salariés, ses sous-traitants et leurs salariés.

Le Fournisseur comme l'AP-HP s'engagent à ne pas divulguer à des tiers les documents, les informations et les renseignements communiqués par l'autre partie à l'occasion de l'exécution du présent Marché, sauf, en cas d'accord écrit donné par l'AP-HP et/ou par le Fournisseur, lorsque les informations sont tombées officiellement dans le domaine public, lorsque les informations sont indiquées par la partie qui les communique à chaque communication, comme n'étant pas confidentielles, lorsque les informations sont diffusées au public préalablement à la notification du Marché ou lorsque les informations sont intégrées dans le produit. Toute communication du Fournisseur vers les tiers, à l'exception des Sociétés Affiliées et sous-traitants du Fournisseur, concernant le Marché et son exécution doit être préalablement soumise à l'accord de l'AP-HP.

Pour Société Affiliées du Fournisseur, on entend toute personne morale, directement ou indirectement contrôlant, contrôlée par ou placée sous contrôle commun avec le Fournisseur. Aux fins de la présente définition, la notion de « contrôle » est celle indiquée à l'article L 233-3 du Code de commerce.

Le Fournisseur veille à ce qu'au cours de l'exécution du Marché, soient respectées la sécurité et la confidentialité des Données et des accès informatiques, de l'AP-HP conformément aux lois et régimes applicables, et notamment la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les dispositions du Code de la propriété intellectuelle applicables aux logiciels et bases de données et celles du Code pénal. Par ailleurs, le Fournisseur s'engage à ne pas conduire l'AP-HP à méconnaître ces dispositions, en procédant à toutes les préconisations utiles en ce sens.

Le Fournisseur s'engage par ailleurs à ne prendre aucune copie des supports, ne pas utiliser les documents à des fins autres que celles spécifiées dans le Marché, ne pas utiliser ou diffuser, sans autorisation préalable écrite de l'AP-HP, à l'exception des Sociétés Affiliées et sous-traitants du Fournisseur, aucune partie ou totalité d'un programme, d'un fichier et/ou d'une donnée détenu(s) par l'AP-HP ou installé(s) sur un élément ou sur un sous-ensemble d'une configuration, d'un matériel ou d'une pièce détachée détenu(s) par l'AP-HP, et/ou aucune documentation détenue par l'AP-HP, à prendre toute mesure, notamment de sécurité matérielle pour assurer la conservation des supports tout au long de la durée du Marché.

Le non-respect de ces dispositions expose le Fournisseur à l'application des mesures prévues à l'article « Résiliation » du CCAP du Marché.

4.3 Sécurité

Le Fournisseur et ses sous-traitants ultérieurs sont tenus de respecter :

- La charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP
- Les prescriptions de la politique générale de sécurité des systèmes d'information (PGSSI) de l'AP-HP annexée au présent Marché ainsi que les directives, les procédures et modes opératoires pris en application de la PGSSI.

Les directives, les procédures et modes opératoires sont communiqués au Fournisseur sur demande motivée par voie électronique dans un délai de 15 jours ouvrés.

Dans tous les cas, le Fournisseur est tenu de fournir à la première demande la documentation nécessaire à la sécurisation de ses prestations et fournitures, la protection des données des bénéficiaires et aux démonstrations du respect de ses obligations.

4.3.1 Accès à la documentation et aux informations par le Fournisseur

L'AP-HP communique au Fournisseur les types d'information et documents auxquelles le Fournisseur pourra accéder dans le cadre de ses prestations.

Par défaut, l'accès aux autres catégories d'information et documents est interdit.

Conformément à la charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP, l'AP-HP met en œuvre des dispositifs d'identification et d'authentification, de contrôle d'accès, et traçabilité pour assurer la sécurité des informations. Le Fournisseur reconnaît être informé que de tels dispositifs sont mis en place. Le Fournisseur et ses sous-traitants ultérieurs informent leurs personnels de la mise en œuvre de ces dispositifs par l'AP-HP. L'AP-HP s'engage à respecter la législation en la matière.

4.3.2 Signalements de failles ou d'incidents de sécurité

Le Fournisseur informe l'AP-HP sous un délai de 72 heures au plus, de la découverte de faille(s) de sécurité ou d'un incident de sécurité impactant l'exécution des prestations.

Toute faille ou incident de sécurité jugé comme significatif par l'AP-HP est obligatoirement notifié aux autorités compétentes (ANS, ANSSI, CNIL...) par l'AP-HP.

Le Fournisseur a obligation d'enregistrer les failles auprès des autorités compétentes, le CERT-FR pour la France, en suivant les réglementations établies. A défaut d'action sous 3 mois, l'AP-HP a la possibilité de se substituer au Fournisseur dans les actions précédentes et de pratiquer une divulgation responsable (annonce de la faille avec embargo pendant au moins 90 jours sur les détails techniques).

4.3.3 Protection contre les logiciels malveillants

Le Fournisseur doit protéger les systèmes d'information utilisés pour la réalisation des Prestations conformément à l'état de l'art en matière d'hygiène informatique et de sécurité, notamment avec des logiciels à jour, un anti-virus activé actualisé au moins toutes les 12 heures.

4.3.4 Gestion des vulnérabilités techniques

Le Fournisseur est tenu de réaliser une gestion des vulnérabilités des systèmes et logiciels qu'il met en œuvre dans le cadre de sa Prestation. Il s'engage à apporter les corrections nécessaires dans des délais raisonnables au vue de la criticité des vulnérabilités et du niveau d'exposition aux menaces. Le Fournisseur informera régulièrement de l'état de l'application des correctifs de sécurité. Toute vulnérabilité pouvant avoir un impact sur la sécurité de l'AP-HP sera notifié au RSSI de l'AP-HP.

4.3.5 Echanges et communications d'informations

L'usage de la messagerie entre le Fournisseur et l'AP-HP se limite à des échanges non confidentiels. Le Fournisseur et l'AP-HP s'engagent à utiliser la plateforme d'échange de fichiers <https://dispose.aphp.fr> conformément aux conditions générales d'utilisation du service lors de la transmission d'informations sensibles et s'interdit de les communiquer par tout autre moyen sauf impossibilité technique.

Le Fournisseur et l'AP-HP s'engagent à limiter l'usage des supports amovibles et à privilégier la plateforme d'échange de fichiers <https://dispose.aphp.fr>.

4.3.6 Accès physiques aux locaux de l'AP-HP

L'AP-HP assure au personnel du Fournisseur appelé à intervenir dans ses locaux, des conditions d'environnement conformes aux normes d'hygiène et de sécurité.

L'AP-HP informe le Fournisseur des consignes de sécurité dans lesdits locaux et emprises.

L'accès aux locaux de l'AP-HP par le Fournisseur est soumis au règlement intérieur (RI) de l'AP-HP.

L'AP-HP tient à jour un registre nominatif des personnels du Fournisseur, autorisés à intervenir dans ses locaux. Seuls les personnels du Fournisseur régulièrement inscrites aux registres peuvent avoir accès aux clés, badges permanents, codes, matériels ou locaux utilisés pour assurer la protection physique des informations et ressources informatiques appartenant à l'AP-HP. Ils s'engagent à les garder secrets, à ne pas les dévoiler ou les laisser à la disposition des tiers, à informer sans délai l'AP-HP en cas de perte ou de vol.

Au cours de ses visites dans les locaux de l'AP-HP, le personnel du Fournisseur ne peut être accompagné d'un tiers sans accord écrit préalable de Personne Publique ou du responsable du site concerné.

Aucune sortie des locaux de l'AP-HP de configurations, de supports numériques ou autres, d'éléments ou sous-ensembles de configuration, de matériel, de pièce détachée et/ou de documentation détenus par l'AP-HP ne peut être faite sans l'autorisation préalable et écrite de l'AP-HP.

Dans le cas des opérations de maintenance (par exemple, réparation matérielle), le Fournisseur doit transmettre au préalable à l'AP-HP un descriptif précisant les dates, la nature des opérations à effectuer et les noms des intervenants.

L'AP-HP veille à la présence effective de l'un de ses personnels qualifiés pendant la durée de l'intervention dudit personnel, de telle sorte que toutes mesures utiles puissent être immédiatement prises en cas d'accident.

Dans le cas de la livraison d'une solution ou de matériel (par exemple : stock informatique, papiers, mobilier), il est toléré que l'accès du bâtiment soit provisoirement ouvert le temps des opérations de livraison. Le personnel de l'AP-HP, à défaut du Fournisseur, est chargé de veiller à surveillance des accès et à la fermeture systématique des accès et des locaux dès la livraison terminée.

Les personnels du Fournisseur s'engagent à :

- Respecter les directives et procédures de sécurité de l'AP-HP
- Informer sans délai la Personne Publique de tout départ, changement de fonction de ses personnels
- A ne pas tenter de contourner les procédures mises en œuvre par l'AP-HP permettant le contrôle des accès autorisés et empêchant les accès non autorisés à ses locaux
- Ne pas essayer de s'introduire dans des locaux non autorisés ou avec d'autres moyens que ceux mis à sa disposition
- Ne pas permettre l'accès aux personnes non autorisées par l'AP-HP dans ses locaux

- Respecter les systèmes de sécurité physique mis en place à l'AP-HP, en particulier fermer systématiquement à clé s'il le peut, les portes derrière lui, même en cas d'absence de courte durée
- Assurer la protection physique du matériel mis à sa disposition
- Restituer tous les objets mis à disposition l'AP-HP permettant l'accès physique aux locaux de l'AP-HP infrastructures à la fin de l'intervention
- Ne réaliser aucune copie ou duplicata des moyens d'accès mis à disposition
- Ne pas entraver le fonctionnement des équipements opérationnels et ceux de sécurité
- Signaler tout défaut de sécurité ou situation qui semblerait anormale.

4.3.7 Vidéo protection

Afin d'assurer la sécurité des biens ou des personnes, certains sites ou lieux sensibles de l'AP-HP ont été équipés de système de vidéo protection. Le Fournisseur reconnaît être informé que de tels systèmes sont mis en place dans les sites et locaux sensibles. Le Fournisseur et ses sous-traitants ultérieurs informent leurs personnels de la mise en œuvre de ces traitements par l'AP-HP. L'AP-HP s'engage à respecter la législation applicable à ce type d'équipement notamment l'affichage obligatoire.

4.3.8 Connexion du matériel du Fournisseur sur les réseaux de l'AP-HP

Dans le cas où le Fournisseur aurait besoin, pour l'exécution de ses prestations, de connecter des matériels informatiques lui appartenant sur le réseau de l'AP-HP, le Fournisseur s'engage à :

- Recueillir préalablement l'accord express de l'AP-HP
- Respecter la charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP, les directives de sécurité et procédures de l'AP-HP
- Ne pas entraver ou de contourner la mise en œuvre et l'action des dispositifs de sécurité de l'AP-HP.
- Garantir que son matériel ne présente aucun risque de compromission ou d'infection par un code informatique malveillant, du réseau informatique de l'AP-HP notamment par une analyse préalable avec un antivirus à jour avant chaque connexion au système d'information de l'AP-HP
- Garantir que cette connexion n'a en aucune manière un impact sur les performances, la disponibilité, l'intégrité et la confidentialité du Système d'Information de Personne Publique
- Chiffrer les données au repos avec un dispositif à l'état de l'art
- Pour les dispositifs ayant une capacité autonome de traitement de l'information (téléphone multifonction, poste de travail informatique...) :
Garantir la présence d'un antivirus à jour et à même de récupérer au moins 1 fois toutes les 24h les dernières signatures antivirales
Utiliser un système d'exploitation dans une version maintenue et à jour des correctifs de sécurité et à même de récupérer et d'installer au moins 1 fois par semaine les derniers correctifs de sécurité
Respecter les contraintes d'adressage MAC/IP
Utiliser des protocoles de communication sans faille connue

Pour les actes d'administration ou d'exploitation qui seraient réalisés par le Fournisseur, le Fournisseur utilise des postes de travail informatiques dédiées à l'exploitation et l'administration isolées des réseaux bureautiques, d'Internet, de la messagerie notamment. Si ces actes sont réalisés depuis les locaux de l'AP-HP, les postes de travail informatiques sont fournis par l'AP-HP.

4.3.9 Accès au système d'information de l'AP-HP par le Fournisseur

Dans le cas où le Fournisseur aurait besoin, pour l'exécution de ses prestations, d'accéder au système d'information de l'AP-HP, le Fournisseur s'engage à :

- Recueillir préalablement l'accord express de l'AP-HP
- Respecter la charte du bon usage du système d'information de l'AP-HP annexe n°16 du règlement intérieur de l'AP-HP, les directives de sécurité et procédures de l'AP-HP
- Identifier nommément ses personnels, en communiquer la liste à l'AP-HP et tenir à jour un registre
- Informer sans délai la Personne Publique de tout départ, changement de fonction de ses personnels
- A ne pas tenter d'entraver ou de contourner les procédures mises en œuvre par l'AP-HP permettant le contrôle des accès autorisés et empêchant les accès non autorisés à son système d'information

- Traiter les moyens d'authentification comme des informations confidentielles
Le Fournisseur est responsable de la gestion et de la confidentialité de ses moyens d'authentification, nécessaires accéder au système d'information de l'AP-HP. Le Fournisseur s'assure notamment que ses personnels ont connaissance et respectent les règles de l'art permettant de préserver la confidentialité de leurs moyens d'authentification.
Le Fournisseur supporte seul les conséquences pouvant résulter de la perte, la divulgation, ou l'utilisation frauduleuse ou illicite des moyens d'authentification fournis à ses personnels, la responsabilité de l'AP-HP ne pouvant en aucun cas être engagée à ce titre.
- Signaler tout défaut de sécurité ou situation qui semblerait anormale.

Le Fournisseur s'engage à informer l'AP-HP sans délai, de toute perte ou divulgation éventuelle des moyens d'authentification, et à procéder immédiatement au renouvellement desdits moyens d'authentification.

Pour les Services relevant de l'Article L1111-8 du code de la santé publique et afin de garantir la confidentialité des données de santé à caractère personnel et leur protection, l'AP-HP met à disposition du Fournisseur des moyens d'authentification conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24 du code de la santé publique.

4.3.10 Interconnexion entre le SI du Fournisseur et le SI de l'AP-HP

Toute interconnexion avec le SI de l'AP-HP doit être préalablement validée par un écrit de l'AP-HP. Cette validation inclut un Dossier d'Architecture Technique, comprenant une matrice de flux, la personne à contacter pour tout événement de sécurité et les exigences de sécurité applicables à cette interconnexion.

4.3.11 Télémaintenance/Téléassistance

Dans le cas où le Fournisseur réalise une prestation de maintenance sur des ressources de l'AP-HP ou sur des ressources du Fournisseur, installées sur le réseau de l'AP-HP, le Fournisseur s'engage à respecter les règles suivantes :

- Obtenir l'accord préalable de l'AP-HP avant chaque opération
- Respecter les directives et procédures de sécurité de l'AP-HP
- A ne pas tenter de contourner les procédures mises en œuvre par l'AP-HP permettant le contrôle des accès autorisés et empêchant les accès non autorisés à son système d'information
- Signaler tout défaut de sécurité ou situation qui semblerait anormale.
- Transmettre systématiquement à l'AP-HP un rapport d'intervention retraçant les opérations menées, les données à caractère personnel accédées, les modifications réalisées sur l'environnement de production et leurs impacts éventuels, et ce quels que soient les composants modifiés (système, applications, middlewares, réseaux...)
- Garantir que son matériel ne présente aucun risque de compromission ou d'infection par un code informatique malveillant, du réseau informatique de l'AP-HP
- Traiter les moyens d'authentification comme des informations confidentielles
- Télé-assister les utilisateurs ou les personnels de l'AP-HP chargés de la mise en œuvre du système d'information conformément aux recommandations de la commission nationale de l'informatique et des libertés (CNIL) depuis les outils mis à disposition par l'AP-HP

4.3.12 Prestation d'externalisation d'une composante du système d'information de l'AP-HP

Le Fournisseur fournira à l'AP-HP la description de l'ensemble des dispositions qu'il s'engage à appliquer en matière de sécurité pour l'exécution du Marché dans un Plan d'Assurance Sécurité (PAS).

Ce PAS présentera notamment la manière dont le Fournisseur répond opérationnellement aux exigences de sécurité du Marché.

Un modèle de plan de PAS est annexé au présent document.

4.3.13 Homologation de sécurité

L'AP-HP met en œuvre une démarche d'intégration de la sécurité dans les projets et procède à une homologation de sécurité conformément au Référentiel Général de Sécurité (RGS).

Le Fournisseur en charge d'un système nécessitant une homologation de sécurité s'engage à communiquer les éléments requis pour instruire l'homologation à l'AP-HP, à appliquer les exigences validées pour l'homologation, à faire évoluer la documentation lors de tout changement du système et à informer l'AP-HP de tout changement significatif pouvant remettre en cause l'homologation.

4.3.14 Certification hébergeur de données de santé de l'AP-HP

Le Fournisseur atteste avoir pris connaissance de la possible intégration de ses prestations dans le périmètre des prestations rendues par l'AP-HP à ses clients et Partenaire relevant de la certification à l'hébergement de données de santé au cours de l'exécution du Marché en application de l'Arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel.

L'AP-HP informe le Fournisseur de cette intégration lors de la phase de consultation.

Le Fournisseur s'engage à ne pas faire obstacle à la mise en œuvre des mesures de sécurité prescrite par le référentiel de certification HDS - Exigences et contrôles - Version 1.1 finale – Mai 2018.

Le Fournisseur informe l'AP-HP des conséquences sur l'exécution de ses prestations.

Le Fournisseur et l'AP-HP peuvent convenir d'un avenant au Marché afin d'adapter les conditions d'exécution des prestations s'il n'a pas été possible d'informer le Fournisseur lors de la phase de consultation.

4.3.15 Système d'information essentiel de l'AP-HP

Le Fournisseur atteste avoir pris connaissance de la possible intégration de ses prestations dans le périmètre des prestations rendues par l'AP-HP à ses clients et Partenaire relevant de la certification à l'hébergement de données de santé au cours de l'exécution du Marché en application de l'Arrêté du 11 juin 2018 portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel.

L'AP-HP informe le Fournisseur de cette intégration lors de la phase de consultation.

Le Fournisseur s'engage à ne pas faire obstacle à la mise en œuvre des mesures de sécurité prescrite par l'Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des Fournisseurs de service numérique

Le Fournisseur informe l'AP-HP des conséquences sur l'exécution de ses prestations.

Le Fournisseur et l'AP-HP peuvent convenir d'un avenant au Marché afin d'adapter les conditions d'exécution des prestations s'il n'a pas été possible d'informer le Fournisseur lors de la phase de consultation.

4.3.16 Certification hébergeur de données de santé du Fournisseur

Le Fournisseur s'engage à être certifié hébergeur de données de santé pour la durée du Marché sur le périmètre des prestations traitant des données de santé relevant de la certification conformément aux règles édictées par l'Agence du Numérique en Santé (ANS).

Le Fournisseur met à disposition de l'AP-HP le certificat ainsi que la déclaration d'applicabilité.

Le Fournisseur informera l'AP-HP de tout risque de perte de cette certification.

4.4 Les exigences fonctionnelles de sécurité

Le présent ensemble de clauses s'applique aux Marchés concernant les prestations de :

- Fourniture de logiciels commerciaux
- Etudes et de mise au point de logiciels spécifiquement conçus et produits pour répondre aux besoins particuliers
- Elaboration de systèmes d'information
- Tierce maintenance applicative.

Le présent ensemble de clauses ne s'applique pas

- Fourniture de matériel informatique ou de télécommunication
- Fourniture de logiciels bureautiques

- Prestations de maintenance ou d'infogérance.

4.4.1 Identification/Authentification

La composante privée du Système accédée doit identifier et authentifier de façon unique les utilisateurs [l'utilisation de comptes partagés n'est pas autorisée]. Il peut exister une composante publique [consultation de données par exemple] ne nécessitant pas d'authentification préalable.

Lorsqu'elles sont nécessaires, l'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la ressource accédée et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussie.

Lorsqu'elles sont nécessaires, l'identification et l'authentification avec l'utilisateur doivent être réalisées au sein d'un environnement sûr. Pour chaque interaction, le Système doit pouvoir établir l'identité de l'utilisateur.

Dans le cas où l'authentification est déportée vers un frontal d'authentification, un chemin sûr [dit de confiance] doit être établi entre le frontal et le Système. La confiance dans ce chemin pourra être atteinte par la mise en place de solutions techniques, procédurales ou organisationnelles. L'utilisation d'un tel frontal ne nuira pas à la mise en place des fonctions de journalisation et d'audit (cf. ci-après).

Lorsque les techniques d'authentification mettent en œuvre des mécanismes cryptographiques, ceux-ci devront présenter un niveau de robustesse au moins équivalent au niveau de robustesse standard défini par l'ANSSI et le Référentiel général de Sécurité (RGS).

Si des moyens d'authentification par mot de passe sont mis en œuvre, le Système doit permettre de contrôler la mise en œuvre d'une politique de gestion rigoureuse : durée de validité du secret, taille minimale et format, gestion des renouvellements et des secrets passés, gestion du nombre de tentatives infructueuses.

Des moyens cryptographiques doivent être mis en œuvre pour garantir la confidentialité et l'intégrité des données d'authentification en transit ou stockées. Ces moyens doivent être cohérents avec la durée de validité retenue pour les paramètres d'authentification et présenter un niveau de robustesse au moins équivalent au niveau de robustesse standard défini par l'ANSSI et le RGS.

Des mesures doivent être mises en œuvre pour garantir l'intégrité des mécanismes d'authentification.

Le Système doit mettre en œuvre une authentification SAML2 ou OPENID CONNECT. L'AP-HP met à disposition du Fournisseur un IDP. Cet IDP utilise une méthode d'authentification par LOGIN/Mot de passe quand l'accès se fait depuis le réseau de l'AP-HP, complété par une authentification à 2 facteurs pour les accès depuis Internet (cas du télétravail).

Si le système traite de données de santé, les moyens d'identification et d'authentification sont conformes au référentiel d'identification électronique des usagers, des acteurs des secteurs sanitaire-médico-social-et-social pour les personnes morales ou physiques de l'ANS.

4.4.2 Contrôle d'accès

Le Système doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur [au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux].

Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un répertoire, un fichier ou une fonction du Progiciel.

Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès au sein du Système.

Il doit également être possible de limiter l'accès en lecture seulement selon les besoins.

Il doit être possible d'accorder les droits d'accès à un objet (répertoire, fichier, fonction) en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès. Seuls des utilisateurs autorisés doivent pouvoir créer de nouveaux comptes utilisateurs, supprimer ou désactiver des comptes utilisateurs existants.

Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à un répertoire, un fichier, ou une fonction du Système, le Système doit vérifier la validité de la demande. Les tentatives d'accès non autorisés doivent être rejetées.

4.4.3 Journalisation / imputabilité

Le Système doit comporter un composant d'imputation qui soit capable de journaliser :

Les tentatives d'identification et d'authentification [données exigées : date, heure, identité fournie par l'utilisateur, identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé, réussite ou échec de la tentative, autorisation de l'utilisateur].

Les actions d'administration [données exigées : Date, heure, identité de l'utilisateur, type de l'action].

En complément, le Système doit pouvoir journaliser certains événements identifiés comme sensibles par les maîtrises d'ouvrage. Les accès à des fichiers, répertoires ou fonctions présentant un caractère sensible [données exigées : Date, heure, identité de l'utilisateur, fonction mise en œuvre, identification de l'objet accédé, type de tentative d'accès, réussite ou échec de la tentative].

Il doit être possible de mettre sélectivement en œuvre l'imputation pour un ou plusieurs utilisateurs.

Les données journalisées ne doivent être accessibles qu'en consultation aux seuls utilisateurs autorisés. Elles doivent être protégées contre tout type de modification ou suppression, afin de garantir l'imputabilité de l'utilisation du Système. Toute action sur une donnée d'imputation devra être tracée

4.4.4 Audit

Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

4.4.5 Protection de l'intégrité du Système

En standard, l'intégrité du Système est assurée par les moyens de contrôle d'intégrité des bases de données et des serveurs mis en place systématiquement par l'AP-HP.

Toute donnée envoyée ou reçue en pièce jointe doit être identifiée et contrôlée. Des précautions doivent être prises afin de prévenir et détecter l'introduction de tout code malveillant par l'intermédiaire des informations transmises, ou pour prévenir toute saturation du Système par l'envoi de pièces de taille anormalement volumineuse. Le contrôle du type et format des données entrantes et sortantes sera assuré par des dispositifs de protection permettant l'analyse de code malveillant, l'analyse de requête autorisée, l'analyse de type et format de données échangées.

4.5 Méthodologie sécurisée d'ingénierie et de développement

Le Fournisseur met en œuvre une méthodologie d'ingénierie et de développement sécurisée pour son Système. Le Fournisseur décrit ses activités et contrôles de sécurité, utilisés en la matière (processus, procédures, outillages, indicateurs). Il s'agit notamment de :

- Formation en lien avec la sécurité des développements
- Définition des exigences de sécurité
- Modélisation de la menace
- Usage d'outils évalués et approuvés
- Gestion des risques de sécurité relatifs à l'usage des logiciels tiers
- Définition des exigences de conception
- Analyse statique et dynamique du code
- Test d'intrusion
- Processus standard de réponse aux défauts et incidents
- Indicateur de pilotage des activités en lien avec la sécurité de l'information
- Rapport de conformité.

Le Fournisseur assurant une prestation de développement s'engage à respecter les bonnes pratiques de sécurité dans le développement, en sus de respecter les exigences de sécurité exprimées dans la documentation sur la sécurité de l'information de l'AP-HP.

4.6 Audits

4.6.1 Audit par le Fournisseur

Agrément relatif à l'auditeur

L'auditeur proposé par le Fournisseur doit être agréé par l'AP-HP. Aucun auditeur ne peut être imposé à l'AP-HP, dans la mesure où il peut présenter un risque de partialité. Il doit être reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Fournisseur, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à l'AP-HP.

Agrément relatif à l'audit

La réalisation de l'audit du Fournisseur est soumise à l'agrément de l'AP-HP. Afin de permettre à l'AP-HP de procéder à l'agrément de l'audit, le Fournisseur fournit à l'AP-HP une lettre de cadrage de l'audit par « lettre recommandée avec avis de réception postale » (ou équivalent) mentionnant notamment : le périmètre des investigations, les limitations, les moyens techniques mis en œuvre, la date proposée, la durée, et toutes informations jugées utiles. Ce document retrace donc notamment l'ensemble des moyens techniques, outils, méthodes... qui sont mis en œuvre lors de l'audit.

L'agrément ne pourra être délivré que dans la mesure où :

- L'audit du Fournisseur ne suscite pas d'impact sur la production de l'AP-HP ni sur le bon fonctionnement de ses services et services associés
- Le Fournisseur respecte un délai de prévenance de deux (2) mois pour soumettre l'agrément de l'audit et de l'auditeur à l'AP-HP.

Modalités complémentaires de délivrance de l'agrément

A réception de l'ensemble des éléments nécessaires pour engager la procédure d'agrément, l'AP-HP dispose d'un (1) mois pour se prononcer sur l'agrément ou le rejet de la demande d'audit.

Modalités liées à la réalisation de l'audit

Le Fournisseur prend en charge l'intégralité des coûts de l'audit, dont notamment la rémunération de l'auditeur interne ou externe, la prise en charge des coûts liés à la mobilisation de ressources humaines internes aux taux horaires desdites personnes...

La personne Publique se réserve la faculté de modifier la date prévue de l'audit :

- Dans la limite de deux (2) reports par demande d'audit

- Avec report de la date de l'audit dans un délai maximal d'un (1) mois suivant la date prévisionnelle agréée.

Responsabilité liée à l'audit

Le Fournisseur engage son entière responsabilité au titre des préjudices qui pourraient naître au détriment de l'AP-HP à l'occasion de l'audit et qui résulteraient, notamment, d'une faute, erreur ou omission de l'auditeur.

Confidentialité liée aux résultats de l'audit

Le Fournisseur s'engage à respecter la plus stricte confidentialité au titre des éléments qu'il serait amené à connaître dans le cadre de l'audit. Il s'engage notamment à ne pas divulguer les résultats de l'audit réalisé à des tiers de l'accord concerné par l'audit.

4.6.2 Audit par l'AP-HP

Sous réserve d'un préavis de dix (10) jours ouvrés, l'AP-HP se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect par le Fournisseur de ses obligations au titre du Marché, notamment par le biais d'un audit.

Le Fournisseur s'engage à répondre aux demandes d'audit de l'AP-HP et effectuées par l'AP-HP elle-même ou par un tiers de confiance qu'elle aura sélectionné, reconnu en tant qu'auditeur indépendant, c'est-à-dire indépendant du Fournisseur, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusion d'audit à l'AP-HP.

Les audits doivent permettre une analyse du respect des obligations contractuelles, réglementaires et légales, notamment : par la vérification de l'ensemble des mesures de sécurité mises en œuvre par le Fournisseur, par la vérification des journaux de localisation des données, de copie et de suppression des données, par l'analyse des mesures mises en place pour supprimer les données, pour prévenir toutes transmissions illégales de données à des juridictions non adéquates ou pour empêcher le transfert de données vers un pays non autorisé. L'audit doit enfin pouvoir permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées sans que cela ne soit détecté et notifié.

Il est toutefois entendu qu'un tel audit ou toute autre forme de contrôle/vérification ne peut en aucun cas porter sur les documents financiers et/ou comptables du Fournisseur ou sur les documents relatifs aux membres du personnel du Fournisseur (sauf accord préalable et éclairé de ces derniers). L'AP-HP s'engage à respecter les obligations de confidentialité qui lui incombent au titre des présentes ainsi que les règles d'accès et de sécurité en vigueur dans les locaux du Fournisseur et se porte fort du respect de ces règles par les membres de son personnel et/ou auditeur externe.

5 ANNEXES

Définitions

Les définitions de l'Article 4 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données s'appliquent aux termes suivants :

« données à caractère personnel », « traitement », « limitation du traitement », « profilage », « pseudonymisation », « fichier », « responsable du traitement », « sous-traitant », « destinataire », « tiers », « consentement », « violation de données à caractère personnel », « données génétiques », « données biométriques », « données concernant la santé », « établissement principal », « représentant », « entreprise », « groupe d'entreprises », « règles d'entreprise contraignantes », « autorité de contrôle », « autorité de contrôle concernée », « traitement transfrontalier », « objection pertinente et motivée », « service de la société de l'information » et « organisation internationale » lorsqu'ils sont cités dans tous les documents et enregistrements.

Les définitions de la norme NF ISO/CEI 27000 FÉVRIER 2011 s'appliquent aux termes suivants :

« acceptation des risques », « actif », « actif informationnel », « action corrective », « action préventive », « analyse des risques », « appréciation des risques », « attaque », « authentification », « confidentialité », « continuité de l'activité », « contrôle d'accès », « critères de risque », « disponibilité », « enregistrement », « estimation des risques », « évaluation des risques », « événement lié à la sécurité de l'information », « fiabilité », « gestion des incidents liés à la sécurité de l'information », « gestion du risque », « incident lié à la sécurité de l'information », « impact », « intégrité », « menace », « mesure de sécurité », « non-répudiation », « objectif de sécurité », « politique », « procédure », « processus », « risque », « risque lié à la sécurité de l'information », « sécurité de l'information », « système de management », « système de management de la sécurité de l'information », « traitement des risques » et « vulnérabilité » lorsqu'ils sont cités dans tous les documents et enregistrement.

Checklist

Cette checklist permet à l'AP-HP d'identifier le contexte d'intervention du Fournisseur.

Elle facilite l'identification par le Fournisseur de ses obligations.

Dans le cadre de l'exécution de ses obligations contractuelles à l'égard de l'AP-HP, le Fournisseur

1. A la qualité de : ☐ Sous-traitant, ☐ Responsable de traitement, ☐ Co-responsable de traitement
2. Traite des données : ☐ Personnelles, ☐ Personnelles de Santé, ☐ Personnelles sensibles autres
3. Accède aux : ☐ locaux, ☐ locaux sensibles, ☐ locaux informatiques
4. Accède aux : ☐ zones sous vidéo protection, ☐ locaux sous vidéo protection
5. Connecte du matériel sur les réseaux de l'AP-HP : ☐ OUI, ☐ NON
6. Accède au système d'information de l'AP-HP : ☐ OUI, ☐ NON
7. Interconnecte son SI avec le SI de l'AP-HP : ☐ OUI, ☐ NON
8. Réalise des prestations de Télémaintenance/Téléassistance : ☐ OUI, ☐ NON
9. Héberge une composante du SI de l'AP-HP : ☐ OUI, ☐ NON
10. Contribue aux homologations de sécurité : ☐ OUI, ☐ NON
11. Intervient sur le périmètre du SI certifié HDS/ISO 27001 de l'AP-HP : ☐ OUI, ☐ NON
12. Intervient sur un Système d'Information Essentiel (SIE) de l'AP-HP : ☐ OUI, ☐ NON

Coordonnées

Délégation à la protection des données

Téléphone : +33 1 40 27 30 00

Courriel à l'adresse électronique : protection.donnees.dsi@aphp.fr

Courrier postal à l'adresse : AP-HP, Déléguee à la protection des données – Direction des Services Numériques - 33, Bd de Picpus, CS 21705, 75571 Paris Cedex 12

Responsable de la sécurité du système d'information

Téléphone : +33 1 40 27 30 00

Courriel à l'adresse électronique : aphp-sigalement-securite@aphp.fr

Courrier postal à l'adresse : AP-HP, RSSI – Direction des Services Numériques - 33, Bd de Picpus, CS 21705, 75571 Paris Cedex 12

Matrice Impact-Gravité

Impact sur les personnes concernées					
Echelle de gravité	I	2	3	4	5
Prise en charge	Prise en charge inchangée	Escalade de la surveillance ou du traitement	Menace vitale	Incapacité	Décès
Continuité de l'hospitalisation	Pas de discontinuité	Discontinuité transitoire	Discontinuité prolongée ou permanente	Complication médicale ou accidentelle liée à la discontinuité	Décès lié à la discontinuité
Vie privée (RGPD)	Pas d'impact	Quelques désagréments surmontés sans difficulté	Désagréments significatifs surmontés avec quelques difficultés	Conséquences significatives surmontées avec de réelles difficultés	Conséquences significatives voire irrémédiables non surmontables
Impact sur l'AP-HP					
Echelle de gravité	I	2	3	4	5
Actifs (informationnels)	Aucune perte d'information	Perte transitoire d'information.	Perte réversible d'information nécessitant d'importants moyens pour leur reconstitution	Perte irréversible d'informations essentielles avec solution de remplacement	Perte irréversible d'informations essentielles sans solution de remplacement
Activité	Aucun impact sur l'activité	Dégradation transitoire de l'activité	Dégradation permanente de l'activité	Arrêt de l'activité, avec solution de remplacement	Arrêt définitif de l'activité
Actifs	Pas de perte financière	Perte ≤ 0,1 %	Perte > 0,1 % et ≤ 1%	Perte > 1 % et ≤ 10 %	Perte > 10 %
Conformité	Observations	Non-conformité mineure	Non-conformité majeure	Interdiction temporaire d'exercer l'activité	Interdiction définitive d'exercer l'activité
Environnement	Aucun impact sur la qualité de l'environnement	Dégradation transitoire de l'environnement local	Dégradation permanente de l'environnement local	Impact à distance transitoire	Impact à distance permanent
Image	Dégrader temporairement l'image de l'AP-HP en interne	Dégrader temporairement l'image de l'AP-HP au niveau régional	Dégrader temporairement la réputation de l'AP-HP au niveau national	Dégrader durablement la réputation de l'AP-HP au niveau national	Dégrader durablement la réputation de l'AP-HP au niveau mondial
Juridique	Absence de réclamation	Réclamation non contentieuse	Risque de réclamation indemnitaire	Réclamation indemnitaire ou risque de réclamation pénale	Réclamation pénale

LES GUIDES DE L'AP-HP

Règlement intérieur

DE L'ASSISTANCE PUBLIQUE-
HÔPITAUX DE PARIS

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

Synthèse des principales règles

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

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

Préambule et objet

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

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

Art.1 Champ d'application de la charte informatique

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

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

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

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

1.2 Système d'information et de communication

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

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

1.3 Cadre législatif et réglementaire

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

- Les droits et libertés reconnus aux utilisateurs du SI de l'AP-HP, notamment la liberté d'expression, les libertés syndicales, et la liberté académique reconnue aux universitaires.
- Le traitement numérique des données, et plus précisément le traitement de données à caractère personnel relatives à la santé et le respect de la vie privée.
- Le droit d'accès des patients et des professionnels de santé aux données médicales.
- L'hébergement de données médicales.
- Le secret professionnel et le secret couvrant les données à caractère personnel relatives à la santé.

- La signature électronique des documents.
- Le secret des correspondances.
- La lutte contre la cybercriminalité.
- La protection des logiciels et des bases de données et le droit d'auteur.

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

Art.2 Les règles générales d'utilisation

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

2.1 Respect des lois, des réglementations et de la déontologie

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

Il est notamment interdit :

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

et l'apologie des crimes, la compromission de mineurs ou leur exposition à des messages à caractère violent ou pornographique, ou toute incitation à la consommation de substances interdites), aux règles d'éthique et de déontologie.

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

2.2 Loi informatique et libertés

La constitution de fichiers informatiques comportant des données à caractère personnel, c'est-à-dire permettant d'identifier directement ou indirectement une personne physique, est encadrée par des règles strictes édictées par la Commission Nationale de l'Informatique et des Libertés (CNIL). La création d'un traitement automatisé de données à caractère personnel suppose ainsi, préalablement à sa mise en œuvre, l'accomplissement d'une formalité auprès du correspondant informatique et libertés de l'AP-HP pour les traitements relevant de son champ de compétence ou de la CNIL le cas échéant. Toute violation des principes et règles adoptés par la CNIL peut engager la responsabilité, y compris pénale, de l'AP-HP et/ou de son auteur. De ce fait, toute personne ou service, souhaitant mettre en place un traitement de données à caractère personnel doit se rapprocher, au préalable, du référent Loi Informatique et Libertés (LIL) de son GH/Site/PIC, généralement rattaché à la DSI des Groupes Hospitaliers.

Art.3 Sécurité des équipements mis à disposition

3.1 Sécurité du poste de travail

La configuration initiale du poste de travail doit être respectée.

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

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

un autre réseau.

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

Les ordinateurs doivent être protégés physiquement.

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

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

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

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

- L'AP-HP met à la disposition des utilisateurs des espaces de stockage afin qu'ils puissent sauvegarder et partager des informations. Les utilisateurs doivent être vigilants quant à l'usage qu'ils font de ces répertoires partagés, et sont responsables des informations qu'ils stockent sur ces ressources. Les documents électroniques et les messages professionnels qui reflètent les activités de l'AP-HP, ou qui formalisent les différentes étapes d'une tâche, d'une décision, d'une procédure, dans le cadre des missions liées à l'activité de l'AP-HP, sont à archiver.
- Les utilisateurs ne doivent jamais effacer, supprimer ou modifier des informations pouvant être nécessaires au bon déroulement des activités et des services rendus par l'AP-HP.
- Ils doivent procéder à des sauvegardes régulières des informations professionnelles, stockées localement sur leur ordinateur, sur les répertoires réseaux et ce, afin d'éviter tout risque de perte d'informations (en cas de défaillance de l'ordinateur par exemple).
- Pour les informations sensibles, l'utilisateur veillera à les stocker dans des répertoires avec des droits réservés aux seules personnes légitimes à y accéder (tels que les répertoires partagés entre les membres d'un service par exemple). En cas de doute, il pourra se renseigner auprès du support SI.

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

3.2 Sécurité des autres moyens du SI

Les supports amovibles doivent être utilisés avec vigilance.

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

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

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

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

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

Les documents sensibles doivent être rapidement récupérés aux imprimantes.

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

Les moyens de télécommunication sont à usage professionnel avant tout.

L'AP-HP met à la disposition des utilisateurs des moyens de télécommunication tels que les télécopieurs (fax) ou les téléphones. Ces moyens de télécommunication sont réservés à des fins strictement professionnelles. Cependant, dans le cadre des nécessités de la vie courante, un usage personnel est toléré à condition qu'il soit conforme à la législation en vigueur et aux bonnes mœurs, et qu'il ne nuise pas aux tâches professionnelles incombant à l'utilisateur ou à la bonne conduite des activités de l'AP-HP. .

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

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

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

Accès à distance et utilisation en situation de mobilité

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

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

Art.4 Droit d'accès et mots de passe

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

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

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

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

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

En cas de départ définitif :

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

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

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

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

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

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

Tous les personnels de l'AP-HP sont soumis au secret professionnel dont le secret médical. Cette obligation revêt une importance toute particulière lorsqu'il s'agit de données à caractère personnel relatives à la santé. Les personnels se doivent de faire preuve d'une discrétion absolue dans l'exercice de leur mission. Un comportement exemplaire est exigé dans toute communication, orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée. Afin de garantir la qualité des services rendus par l'AP-HP et l'intégrité de son SI, chaque utilisateur ne doit accéder qu'aux seules informations nécessaires à la réalisation de son activité professionnelle et dans le respect des principes de confidentialité. Les informations consultées dans le cadre de tâches professionnelles ne doivent être utilisées qu'à ce titre.

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

Art.5 Utilisation d'Internet

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

Internet est à usage professionnel avant tout.

L'AP-HP met à la disposition des utilisateurs l'accès à Internet. Cet accès est réservé à des fins strictement professionnelles. Cependant, dans le cadre des nécessités de la vie courante, un usage personnel (réservation de billets de trains, consultation de plans ou horaires, appels d'urgence...) est toléré, à condition qu'il soit conforme à la législation en vigueur et aux bonnes mœurs, et qu'il ne nuise pas aux tâches professionnelles incombant à l'utilisateur ou à la bonne conduite des activités de l'AP-HP.

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

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

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

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

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

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

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

Gestion des communications chiffrées.

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

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

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

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

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

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

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

Art.6 Utilisation de la messagerie électronique

La messagerie électronique est à usage professionnel avant tout.

L'AP-HP met à la disposition des utilisateurs une messagerie électronique. Cette messagerie est réservée à des fins strictement professionnelles. Cependant, dans le cadre des nécessités de la vie courante, un usage personnel est toléré à condition qu'il soit conforme à la législation en vigueur et aux bonnes mœurs, et qu'il ne nuise pas aux tâches professionnelles incombant à l'utilisateur et à la bonne conduite des activités de l'AP-HP. En outre, cet usage ne doit pas compromettre la sécurité du Système d'Information et la disponibilité des services de messagerie, mis à la disposition des utilisateurs.

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

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

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

Art.7 Remontées des incidents par les utilisateurs

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

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

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

Art.8 Tracabilité, procédures de contrôle et sanctions

8.1 Traçabilité et procédures de contrôle

Conformément à la réglementation, l'AP-HP trace et contrôle les communications et l'usage de ses équipements pour, notamment :

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

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

- L'identifiant de l'utilisateur ayant déclenché l'opération ;
- L'heure de la connexion ;
- Le système auquel il est accédé ;
- Le type d'opération réalisée ;
- Les informations ajoutées, modifiées ou supprimées des bases de données en réseau et/ ou des applications de l'AP-HP ;
- La durée de la connexion (notamment pour l'accès Internet).

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

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

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

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

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

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

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

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

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

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

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

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

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

8.1 Sanctions

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

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

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

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

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

- Information de la commission centrale et des commissions locales des soins infirmiers, de rééducation et 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.