

DEMANDE D'ACCÈS POUR UN UTILISATEUR NON SALARIÉ AP-HP

Document à remplir par le responsable et à envoyer daté et signé au support informatique ou au bureau de la Sécurité Générale du GHU / site

Référence de la demande  (trigramme du site_JJMMAAAA_initiales de l'utilisateur) _____

Exemple : SAP_01072020_DK

☐ Création

☐ Modification

☐ Désactivation

☐ Renouvellement

L'utilisateur a-t-il besoin d'accéder au SI ? (Compte AD) 

OUI

NON

☐
☐

**Création automatique d'un compte nominatif Active Directory permettant à minima l'ouverture d'une session Windows nominative. La création d'un compte non salarié (7M) avec accès SI doit être encadrée au travers d'une convention ou du contrat de prestation en application de la Charte de bon usage du Système d'Information.*

La demande concerne uniquement les accès physiques ? 

OUI

NON

☐
☐

**Création d'un compte non salarié sans accès SI pour l'attribution d'une carte d'accès nominative.*

Coordonnées du responsable de la demande (Cadre, chef de service, directeur) *¹

Etablissement  :	Service (UG/UF)  :
Nom  :	Prénom  :
Matricule (APH)  :	Fonction  :
Mail (aphp.fr) :	Téléphone :

¹ La personne à l'origine de la demande est responsable de la gestion des accès et devra déclarer impérativement tout changement concernant l'utilisateur.

 Les champs indiqués par ce point sont obligatoires.

Coordonnées du bénéficiaire

Civilité ⓘ :	Matricule 7M ⓘ : (uniquement pour renouvellement)
Nom ⓘ :	Prénom ⓘ :
Service (UG/UF) ⓘ :	Organisme (Société) ⓘ :
Fonction ⓘ :	Secteur (PM ou PNM) ⓘ :
Mail (professionnel) non APHP ⓘ :	Téléphone :

Motif de la demande ⓘ

Date d'arrivée ⓘ :	Date de départ ⓘ :
--------------------	--------------------

La durée de l'accès demandé ne peut excéder 3 ans.

L'utilisateur a-t-il besoin d'une messagerie AP- HP ? (-ext@aphp.fr) OUI NON
☐ ☐

L'utilisateur a-t-il besoin d'accéder à d'autres applications ? OUI NON
☐ ☐

Si OUI, préciser : _____

Merci de sélectionner la carte correspondant à la demande

(Toute nouvelle demande de création de compte donne droit à une carte d'accès pour l'identification physique, voir le bureau local des cartes professionnelles ou de la sécurité générale pour l'attribution.)

CAN (Carte d'Accès Nominative) ☐

**Les cartes d'accès nominatives sont attribuées aux personnels non-salariés intervenant régulièrement à l'AP-HP [besoin d'accès ponctuel < à 14 jours] ou pour les demandes d'accès au logement sur sites ou au SELF pour les retraités. La carte est remise à l'intéressé pour la durée de la mission, du contrat ou du temps de présence estimé (validité maximale : 3 ans). Les intervenants temporaires [besoin d'accès ponctuel < à 6 jours] se voient attribuer des cartes d'accès temporaires en cas de besoin. Carte remise chaque jour à l'intéressé contre un document officiel.*

CPE dérogatoire (Carte Professionnel d'Etablissement) ☐

**Uniquement pour les prestataires (Profils SI).*

Conformément au règlement intérieur de l'AP-HP, la commande de carte CPE dérogatoire n'est autorisée que pour les prestataires de la DSI ou des DSILs et n'est justifiée que si l'utilisateur non salarié a besoin de la carte CPE dans l'exercice de ses missions : usage de l'authentification forte (SSO), accès aux télé-services ANS, etc. selon les conditions définies par le contrat de prestation liant la société prestataire à l'AP-HP ou la convention dans le cas d'un organisme partenaire.

ⓘ Les champs indiqués par ce point sont obligatoires.

Confidentialité

Toute information ou document communiqué par la Personne Publique au Bénéficiaire, sous quelque forme que ce soit, devra être considéré comme ayant un caractère confidentiel.

Ne constituent pas des informations confidentielles les informations qui :

- (i) sont déjà connues du Titulaire qui les reçoit préalablement à la date de leur divulgation par la Personne Publique.
 - (ii) sont disponibles dans le domaine public lors de leur divulgation ou tombent ultérieurement dans le domaine public, sans manquement aux stipulations de ce Contrat.
 - (iii) sont communiquées par un tiers à titre non confidentiel au Titulaire, dès lors que ce tiers n'est pas lié à l'autre partie par une quelconque obligation de confidentialité.
 - (iv) sont développées de manière indépendante par le Titulaire qui les reçoit, en dehors de tout manquement aux stipulations de ce Contrat.
- Toute donnée dont le Bénéficiaire a connaissance à l'occasion de l'exécution sa prestation est strictement couverte par le secret professionnel (article 226-13 du Code pénal).

Le Bénéficiaire veille à ce qu'au cours de l'exécution de ses prestations, soient respectées la sécurité et la confidentialité des données et des accès informatiques de la Personne Publique conformément aux lois et régimes applicables, et notamment conformément à la loi n° 78-17 du 6 janvier 1978 modifiée par la Loi du 6 août 2004 relative à l'informatique, aux fichiers et aux libertés, (article 29) et aux dispositions du code pénal en vigueur.

A ce titre, le Bénéficiaire s'engage :

1. à n'utiliser les informations et documents délivrés par la Personne Publique qu'à sa demande exclusive et pour la finalité du marché cité en référence du présent formulaire.
2. à ne pas divulguer à des tiers, à titre gratuit ou onéreux, et sous quelque forme que ce soit, les informations et documents communiqués par la Personne Publique à l'occasion de l'exécution du marché cité en référence du présent formulaire.
3. à prendre toutes les mesures pour que lesdites données ne puissent être accessibles à d'autres personnes que les personnels attachés à leur traitement et à leur analyse. Ces derniers seront sensibilisés au caractère stratégique des informations et documents confiés et liés au Bénéficiaire par un engagement de confidentialité.
4. à ne pas procéder à des copies, utilisations ou diffusion de partie ou totalité d'un fichier et/ou d'une donnée détenus par la Personne Publique ou installés sur une configuration, sur un support, sur un élément ou sur un sous-ensemble d'une configuration détenus par celle-ci, à l'exception des copies, utilisations ou diffusion nécessaires à l'exécution d'une prestation prévue au marché cité en référence du présent formulaire, auquel cas l'accord de la Personne Publique est nécessaire.
5. à ne pas sortir du lieu d'hébergement des configurations, des supports numériques ou d'autres, d'éléments ou sous-ensembles d'une configuration, d'un matériel, ou d'une documentation détenue par la Personne Publique sans l'autorisation préalable et écrite de celle-ci.
6. En qualité de « sous-traitant » au sens de la loi n° 78-17 du 6 janvier 1978 en vigueur, à effectuer tout traitement de données personnelles dans le respect des lois et règlements applicables en matière de protection des données personnelles.

A chiffrer les informations présentes sur l'équipement tiers avec un logiciel de chiffrement ayant fait l'objet d'une certification CSPN par l'ANSSI (<http://www.ssi.gouv.fr/fr/certification-qualification/cspn/>).

Le Bénéficiaire sera responsable vis-à-vis de la Personne Publique de la perte de documents remis sous quelque forme que ce soit, ou de la divulgation volontaire ou involontaire d'informations communiquées. Le Bénéficiaire s'engage, à ce titre, à aviser sans délai la Personne Publique de toute disparition, ainsi que de tout incident pouvant révéler un risque de violation des présentes obligations.

Le Bénéficiaire doit procéder à la destruction ou à la restitution de tous les fichiers manuels ou informatisés stockant les informations saisies, à l'échéance du marché ou sur ordre de la Personne Publique.

Ces dispositions s'appliquent au Bénéficiaire mais également à tout opérateur économique intervenant pour le compte ou en partenariat avec le Bénéficiaire (cotraitants et sous-traitants notamment).

La Personne Publique se réserve le droit de procéder à toute vérification qui lui paraîtrait nécessaire pour constater le respect des obligations précitées par le Bénéficiaire. Il est toutefois entendu entre les parties 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 Titulaire ou sur les documents relatifs aux membres du personnel du Titulaire (sauf accord préalable et éclairé de ces derniers). La Personne Publique 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 Titulaire et se porte fort du respect de ces règles par les membres de son personnel et/ou auditeur externe.

En cas de non-respect des dispositions précitées, la responsabilité du Bénéficiaire peut également être engagée sur la base des dispositions des articles 226-5 et 226-17 du code pénal.

Télémaintenance

Chaque opération de maintenance devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants, transmis à la Personne Publique.

En cas de télémaintenance permettant l'accès à distance aux fichiers de la Personne Publique, le Bénéficiaire prendra toutes dispositions afin de permettre à la Personne Publique d'identifier la provenance de chaque intervention extérieure. A cette fin, le Bénéficiaire s'engage à obtenir l'accord préalable de la Personne Publique avant chaque opération de télémaintenance dont elle prendrait l'initiative.

Des registres sont établis sous la responsabilité du Bénéficiaire, mentionnant les dates et nature détaillées des interventions de télémaintenance.

En cas de manquement, l'autorisation de connexion pourra être révoquée sans préavis et sans préjudice d'éventuelles poursuites.

La Personne Publique se réserve le droit d'exiger du Titulaire, sans versement d'aucune indemnité, le remplacement immédiat du Bénéficiaire qui aurait contrevenu aux règles précédemment édictées.

La Personne Publique pourra prononcer la résiliation immédiate du marché, sans indemnité en faveur du Titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées.

Synthèse de la charte de bon usage du système d'information de l'AP-HP

PREAMBULE ET OBJET

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 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'APHP, validée par la Direction Générale. Elle constitue une annexe au règlement intérieur.

ARTICLE 1 : CHAMP D'APPLICATION DE LA CHARTE INFORMATIQUE

La Charte informatique s'applique à l'ensemble des utilisateurs du Système d'Information de l'AP-HP.

Les règles de la Charte informatique doivent, être prises en compte par le personnel des entités sous-traitantes et des partenaires externes accédant au SI de l'AP-HP.

ARTICLE 2 : REGLES GENERALES D'UTILISATION

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

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.

ARTICLE 3 : SECURITE DES EQUIPEMENTS MIS A DISPOSITION

La configuration du matériel de l'AP-HP a été étudiée afin de garantir le bon fonctionnement et la sécurité du Système d'Information et de ce fait 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 téléphones portables et smartphones doivent être protégés par un code.

ARTICLE 4 : DROIT D'ACCES ET MOTS DE PASSE

Les droits d'accès à tout ou partie du SI de l'AP-HP reposent sur un compte d'accès strictement personnel. 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 et soient révoqués ou désactivés à leur départ.

L'utilisateur doit définir un mot de passe complexe et doit veiller à le modifier régulièrement afin d'éviter toute usurpation de son identité.

Tous les personnels de l'AP-HP sont soumis au secret professionnel dont le secret médical et se doivent de faire preuve d'une discrétion absolue dans l'exercice de leur mission.

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.

ARTICLE 5 : UTILISATION D'INTERNET

L'AP-HP met à la disposition des utilisateurs un accès à Internet réservé à des fins strictement professionnelles. 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.

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.

ARTICLE 6 : UTILISATION DE LA MESSAGERIE ELECTRONIQUE

L'AP-HP met à la disposition des utilisateurs une messagerie électronique. Cette messagerie est réservée à des fins strictement professionnelles.

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 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.

L'utilisation d'une messagerie sécurisée est obligatoire pour tout échange de données à caractère personnel relatives à la santé.

ARTICLE 7 : REMONTEE DES INCIDENTS PAR LES UTILISATEURS

Toute anomalie suspectée ou avérée concernant le SI de l'AP-HP, 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.

ARTICLE 8 : TRAÇABILITE, PROCEDURES DE CONTROLE ET SANCTIONS

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

- Contrôler le volume d'utilisation de la ressource, détecter des anomalies afin d'améliorer la qualité de service, faire évoluer les équipements en fonction des besoins
- Vérifier que les règles en matière de sécurité des Systèmes d'Information 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.

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.

Toutes les données, tous les messages électroniques, tous les SMS émis, reçus ou stockés sur le Système d'Information de l'APHP ou sur un matériel ou un système informatique fourni par l'APHP non identifiés comme étant personnels seront, par défaut, considérés comme étant professionnels. En cas de risque particulier susceptible de porter préjudice à l'APHP, 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.

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.

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

Conformément à l'article L. 6143-7 du Code de la santé publique, le Directeur Général de l'AP-HP a arrêté la présente charte d'utilisation du Système d'Information après soumission à la commission centrale et aux commissions locales de soins infirmiers de rééducation et médicotextuelles, information des doyens des UFR de médecine, consultations des instances représentatives centrale de l'assistance publique Hôpitaux de Paris, soumission au conseil de surveillance et au directoire. La Charte d'utilisation du Système d'Information est susceptible d'être modifiée en fonction du contexte législatif et réglementaire.

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

L'AP-HP a mis en place un annuaire technique, ACTIVE DIRECTORY (AD), qui permet de centraliser des informations relatives aux utilisateurs et aux ressources informatiques de l'APHP en fournissant des mécanismes d'identification et d'authentification, tout en sécurisant l'accès aux données. Tout agent en position statutaire AC (activité) a potentiellement accès au système d'information.

Les habilitations aux différentes applications sont demandées par le supérieur hiérarchique en fonction des nécessités de service.

Le compte de messagerie de l'utilisateur sera désactivé **2 mois** après la date du départ (**1 mois** pour le personnel non médical) saisie dans HRACCESS, puis supprimé automatiquement un an après.

Les cas d'exceptions seront traités par les Directions des GH/Sites/PIC et la DSI locale ou par le cabinet du secrétariat général.

La charte de bon usage du système d'information est publiée sur le site Intranet de l'AP-HP à l'adresse <http://dsi.aphp.fr/charte-de-bon-usage-du-systeme-dinformation/>. Le responsable de la demande et l'utilisateur reconnaissent en avoir pris connaissance.

<u>Visa du responsable de la demande</u>	<u>Visa du bénéficiaire</u>
Nom et Prénom :	Nom et Prénom :
Date :	Date :
Signature :	Signature :
<i>La signature est obligatoire.</i>	<i>La signature est obligatoire.</i>

Ce document est un élément de preuve, d'engagement et de confidentialité. Il doit être conservé et pourra être demandé en cas d'audit.