ANNEXE N°0 au CCAPC

MODALITES D'ACCES AUX DONNEES DE SANTE A CARACTERE PERSONNEL SUR LA PLATEFORME DES DONNEES HOSPITALIERES DE L'ATIH

ARTICLE 1 - OBJET

Dans le cadre de l'exécution du présent accord-cadre, le titulaire (« **organisme demandeur** ») est susceptible de traiter des données de santé à caractère personnel pour le compte de l'ATIH.

Le personnel du titulaire (« **les utilisateurs** ») accèdera aux données de santé à caractère personnel mises à disposition par l'ATIH dans les conditions précisées ci-après.

ARTICLE 2 - MODALITÉS DE MISE EN ŒUVRE DE L'ACCES AU SYSTEME

L'accès aux données est réalisé par l'intermédiaire d'une connexion internet sécurisée (protocole HTTPS) avec une authentification forte liée à un système OTP (mot de passe à usage unique) délivré par un matériel fourni par l'ATIH à un utilisateur spécifique (jeton).

La connexion à cette machine virtuelle permet elle-même la connexion à un serveur SAS, à l'aide du logiciel SAS Enterprise Guide. Seul l'environnement SAS est disponible dans cette solution dans un premier temps.

La traçabilité est assurée par un mécanisme d'audit (système de log) de tous les traitements SAS réalisés, ainsi que par la mise en place d'un mécanisme de surveillance informatique (« keylogger ») permettant d'enregistrer toutes les actions réalisées par l'utilisateur. Les entrées ou sorties de données sont autorisées sans contrainte *a priori*, mais peuvent être tracées *a posteriori* grâce aux mécanismes mis en place.

Confidentialité des données

Les données de santé à caractère personnel mises à disposition par l'ATIH que va traiter **« le demandeur »** sont des données confidentielles.
Les traitements de ces informations réalisés par le demandeur ne pourront avoir d'autres fins que celles prévues par l'autorisation CNIL qu'il a obtenu, et dans le respect des textes législatifs et réglementaires relatifs aux données de santé, à la protection des données à caractère personnel et au secret professionnel tel que défini par les articles 226-13 et 226-14 du code pénal.
Dans le cadre de la solution de traitement fournie par l'ATIH, les sorties de données sont possibles, mais il ne peut s'agir que de données anonymes. Les « données anonymes » s'entendent comme des données statistiques agrégées constituées de telle sorte que l'identification, directe ou indirecte, des personnes concernées y est impossible.

Obtention des dispositifs de connexion

L'ATIH a mis en place un système d'authentification forte, basée sur la fourniture aux utilisateurs d'un dispositif (token) permettant la génération d'un OTP (One Time Password) qui permet à l'utilisateur de se connecter. De plus, la connexion à la plateforme requiert un mot de passe personnel respectant les normes de sécurité standards que l'utilisateur devra obligatoirement changer tous les six mois.

Afin d'obtenir le dispositif de génération des OTP (token) :

- le demandeur doit renseigner l'annexe 1 « Déclaration d'un nouvel organisme », permettant d'identifier au sein de l'organisme un utilisateur référent pour la gestion des échanges avec l'ATIH, ainsi qu'un suppléant en cas d'absence du référent.

- Il doit ensuite renseigner autant d'exemplaires de l'annexe 2 « Demande de livraison de jeton d'accès sécurisé (token) » que d'utilisateurs devant réaliser des traitements sur le serveur de l'ATIH (y compris l'utilisateur référent et son suppléant). Cette annexe inclut les engagements individuels de chaque utilisateur.

- Le demandeur doit ensuite renvoyer à l'ATIH les annexes 1 et 2 renseignées et signées. Une fois reçues, l'ATIH envoie, en recommandé avec accusé de réception, à l'utilisateur référent (ou à son suppléant) :
  - les dispositifs de connexion (token)
  - les bordereaux de transfert, un par utilisateur, présentés en annexe 3.

- Chaque bordereau de transfert indiquant la bonne réception des dispositifs de connexion (token), devra être signé par l'utilisateur, l'utilisateur référent (ou son suppléant) et le responsable légal de l'organisme demandeur, et renvoyé à l'ATIH par voie postale.

- Dès réception de ces bordereaux dûment renseignés, l'ATIH envoie par courrier électronique à chaque utilisateur un mot de passe initial, qui devra être obligatoirement changé à la première connexion ainsi qu'une notice précisant les conditions d'utilisation du jeton d'accès sécurisé.

Le dispositif de connexion (token) est strictement personnel, il ne doit en aucune manière être cédé à un autre utilisateur.

En cas de perte, vol, dégradation du jeton, l'organisme sera facturé à hauteur de 200 euros par jeton.

Gestion des utilisateurs

« Le demandeur » s'engage à gérer au plus près les utilisateurs détenteurs de dispositif de connexion. L'utilisateur référent doit informer l'ATIH dans le plus bref délai du départ d'un salarié autorisé à utiliser les données de santé à caractère personnel mises à disposition par l'ATIH et retourner le dispositif de connexion (token) du salarié en question dans la quinzaine qui suit son départ par courrier recommandé avec accusé de réception.

Si le remplaçant du salarié « partant » doit également disposer d'un dispositif de connexion, il est fortement conseillé de joindre l'annexe 2 relative à sa demande renseignée et signée au renvoi du dispositif de connexion du salarié partant.

Aucun nouveau dispositif de connexion ne sera délivré avant réception du dispositif du salarié partant.

En cas de demande d'ajout d'un nouvel utilisateur, le bordereau présenté en annexe 2 doit-être renvoyé dûment signé.

En cas de départ de l'utilisateur référent, le responsable légal du demandeur doit en désigner un nouveau à l'aide du bordereau présenté en annexe 1.

L'ATIH établira des statistiques de connexions une fois par an afin de déterminer les fréquences de connexions des utilisateurs. Ces statistiques seront remises à l'utilisateur référent. En cas d'absence de connexion de plus de 3 mois, une demande de confirmation de maintien de l'utilisateur sera réalisée par l'ATIH.

ARTICLE 4 – ROLE DE L'ATIH

Disponibilité et sécurisation des données

L'ATIH s'engage à mettre à disposition un serveur en état de marche permettant de réaliser les traitements. Ce serveur sera opérationnel du lundi matin 9h au samedi midi (jours fériés inclus).
Les données de santé à caractère personnel mises à disposition par l'ATIH ainsi que l'ensemble des référentiels seront mis à jour en fonction de leur disponibilité, et en fonction de l'autorisation du demandeur.
Les espaces de travail des utilisateurs sont sauvegardés selon plusieurs périodicités :

- quotidienne avec une durée de conservation de 5 jours,
- hebdomadaire avec une durée de conservation de 5 semaines,
- mensuelle avec une durée de conservation de 12 mois,
- annuelle avec une durée de conservation de 10 ans.

Traçabilité des traitements

Le système d'audit SAS (logs) est activé sur le serveur. Les logs de l'ensemble des traitements réalisés sur le serveur sont conservés pendant une durée de 5 ans maximum, permettant ainsi d'opérer des contrôles.

L'ensemble des organismes demandeurs seront informés de toutes modifications opérées par rapport à cette procédure initiale pendant la durée du marché.

Suivi des sessions de connexion

L'ATIH a installé un logiciel permettant d'enregistrer toutes les actions réalisées par les utilisateurs sur leur session Windows distante. Les actions de récupération de données sont particulièrement suivies. D'autres alertes pourront être mises en œuvre dans le cadre de contrôles.

Les utilisateurs sont informés que leurs actions sont tracées.

En cas de constatation de manquement aux engagements de confidentialité, ou d'utilisation inappropriée des données ou des matériels par un utilisateur, l'ATIH contactera l'utilisateur référent ainsi que le directeur de l'organisme demandeur, afin de prendre les mesures nécessaires.

Les dispositifs de connexions devront être retournés à l'ATIH, dans la quinzaine suivant la date de fin d'exécution des prestations objet d'un bon de commande ou, le cas échéant, suivant la date d'échéance ou de prise d'effet de la résiliation de l'accord-cadre.

ARTICLE 5 – FORMULAIRES A COMPLETER ET A TRANSMETTRE A L'ATIH

- L'annexe 1 « Déclaration d'un nouvel organisme »
- L'annexe 2 « Demande de livraison de jeton d'accès sécurisé (TOKEN) »
- L'annexe 3 « Bordereau de transfert de jeton sécurisé »