Plan Assurance Sécurité de la vérification de conformité du label « e-santé Logiciel Maisons et Centres de santé V2 »

Dans le cadre de la vérification de conformité au label « e-santé Logiciel Maisons et Centres de santé V2 » des logiciels, l'ASIP Santé réalise deux types d'opérations :

- des visites de conformité des logiciels labellisés chez l'éditeur de logiciel ou tout autre endroit déterminé en accord avec lui, sur un système de démonstration fourni par l'éditeur de logiciel et ne comportant aucune données de santé à caractère personnel.

- des audits de ces logiciels sur un système en production chez un client utilisateur de la solution auditée ; le système comporte dans ce cas des données à caractère personnel ; dans la mesure du possible, les tests sont réalisés sur un patient fictif ; il peut arriver que certaines vérifications nécessitent l'affichage de données de santé à caractère personnel. En aucun cas, l'auditeur ne réalise de copie d'écran ou ne note les informations de santé à caractère personnel présente à l'écran.

Dans les deux cas l'auditeur de l'ASIP Santé n'intervient à aucun moment sur le poste de travail et ne manipule lui-même le logiciel objet de la vérification.

Les visites de conformité complémentaires et les audits peuvent être réalisés au travers d'un outil de prise en main à distance d'un poste de travail. Dans ce second cas, seul l'affichage déporté du logiciel est utilisé.

Soucieuse de réaliser ces opérations dans les meilleures conditions de sécurité possibles, l'ASIP Santé met en œuvre le plan d'assurance sécurité suivant.

CONTROLE DE L'INTERVENTION

Avant toute intervention sur un système en production, le professionnel de santé en charge de gérer l'audit avec l'ASIP Santé est informé par courrier de la date et de l'heure de l'intervention, de la procédure mise en œuvre dans le cadre de cet audit et que l'acceptation de l'audit emporte l'acceptation de cette procédure.

L'éditeur de logiciel dans le cadre de la visite de conformité ou le professionnel de santé dans le cadre des audits sont responsables des manipulations effectuées sur le logiciel, l'auditeur de l'ASIP Santé n'intervenant à aucun moment sur le poste de travail au-delà du déport de l'affichage dans le cadre d'une intervention à distance.

SELECTION DES INTERVENANTS

Les personnels réalisant les visites de conformité et les audits sont des personnels disposant de fiches de poste décrivant leurs missions au regard du programme de labellisation.

Comme tous les personnels de l'ASIP Santé, ils s'engagent à respecter la politique de sécurité de l'information de l'agence ainsi que la charte d'utilisation des ressources informatiques. Ces documents abordent la thématique de responsabilité des acteurs vis-à-vis des informations qui leur sont confiées et qu'ils traitent. Ainsi, chaque acteur doit-il prendre en considération le niveau de sensibilité des informations qui lui sont confiées. Par ailleurs, la classification des ressources mise en œuvre par l'ASIP Santé oblige chaque propriétaire des informations traitées à en assurer la protection sur l'ensemble de son cycle de vie.

Dans le cadre des opérations de visite de conformité et d'audit, le contrat de travail des personnes chargées de ces opérations comporte une clause de confidentialité et secret professionnel. Cette clause informe les opérateurs sur la sécurité de la prestation, les sensibilise et les engage en termes de confidentialité vis-à-vis leurs missions et sans limitation de durée.

Enfin, afin de maintenir le niveau de mobilisation des personnels de l'ASIP Santé sur la protection des données confidentielles, des sessions de sensibilisation à la sécurité sont régulièrement réalisées au sein de l'agence.

SECURISATION DES POSTES DE TRAVAIL

Configuration des postes

Les utilisateurs ne sont pas autorisés à installer des logiciels ne faisant pas partie de la configuration par défaut. Le parc logiciel est contrôlé automatiquement. Le déploiement de logiciels supplémentaires nécessite une validation hiérarchique.

Les postes utilisés pour la visite de conformité ou l'audit à distance sont maintenus à jour en termes de logiciel et de système d'exploitation.

Ils sont tous équipés d'un logiciel anti-virus à jour.

Gestion des droits

Tout le personnel de l'ASIP Santé applique une politique de gestion des mots de passe conforme aux recommandations de la CNIL. Les mots de passe des administrateurs utilisent une complexité de 10 caractères choisis parmi 4 classes de caractère. Cette politique de gestion des mots de passe est appliquée à l'outil de prise en main à distance. Les mots de passe sont renouvelés périodiquement tous les 90 jours avec un historique de 12 mots de passe (c.à.d. un utilisateur ne peut pas choisir comme nouveau mot de passe lors d'un renouvellement, un des 12 mots de passe qu'il a déjà utilisé précédemment).

La fourniture de compte administrateurs aux personnels nécessitant ces droits est réalisée avec validation du RSSI (Responsable Sécurité du Système d'Information). La liste des comptes administrateurs est revue régulièrement.

Paramétrage des postes

Les postes utilisateurs sont paramétrés pour se mettre en veille automatiquement au bout de 60 minutes en verrouillant la session utilisateur.

Réseau

Le réseau de l'ASIP Santé est segmenté logiquement afin d'assurer le cloisonnement technique entre les différents environnements de l'Agence. Les postes du service opérant la prise en main à distance sont isolés des autres services.

Tous les flux réseaux de l'agence sont contrôlés par un Firewall. Seuls les flux nécessaires à chaque service sont autorisés.

Traçabilité des connexions

Toutes les connexions réalisées par les intervenants sont tracées par l'outil de prise en main à distance.
Par ailleurs, tous les flux réseaux sont tracés par le Firewall.

Sauvegarde et archivage

Toutes les données de traçabilité des connexions réalisées sont sauvegardées à des fins de gestion d'incident. Le Correspondant Informatique et Liberté (CIL) de l'ASIP Santé assure le suivi des délais de conservation des données en fonction de leur sensibilité et réalise les déclarations adéquates auprès de la CNIL.

SECURISATION DES LOCAUX

Les opérations de visite de conformité ou d'audit par prise en main à distance du poste de travail de l'éditeur ou du professionnel de santé sont réalisées à partir des locaux de l'ASIP Santé. Le site de l'ASIP Santé est sécurisé par un contrôle d'accès par cartes à puce CPA. Seuls les personnels de l'ASIP Santé sont habilités à accéder aux locaux.
Les bureaux de l'ASIP sont également fermés à clés et seuls les personnels de chaque bureau ainsi que les services de sécurité disposent de la clé permettant d'y accéder.

ORGANISATION DE LA SECURITE

Gestion des incidents

L'ASIP Santé dispose d'une organisation qui permet de gérer les incidents opérationnels ou de sécurité pouvant se produire sur ses activités. Les membres d'une cellule de crise sont désignés. Le fonctionnement de la cellule de crise est formalisé. Les processus de gestion des incidents sont formalisés. L'ASIP Santé dispose de médecin pouvant intervenir en cas d'incident concernant la divulgation de données de santé lors d'une vérification de conformité ou d'un audit.

Continuité de service

La compétence nécessaire à la réalisation des visites de conformité et des audits est partagée par plusieurs acteurs afin de garantir la continuité d'activité en cas de défaillance humaine.

Conformité

L'ASIP Santé réalise régulièrement des audits de ses services afin de valider leur conformité vis-à-vis des politiques de l'agence. En cas de non-conformité, des plans de remédiation sont définis afin de suivre la mise en conformité des défaillances identifiées.

Les personnes concernées par les opérations de visite de conformité ou d'audit par prise en main à distance du poste de travail de l'éditeur ou du professionnel de santé peuvent diligenter les services compétents afin d'auditer les services d'intervention fournis par l'ASIP Santé.