Sécurité des systèmes d'information

Un document de la Commission Système d'Information

Aujourd'hui, la sécurité des données est un enjeu majeur pour les Services de Santé au travail qui mettent à disposition de leurs personnels des moyens informatiques, téléphoniques et de communication pour leur permettre de travailler au quotidien. Or, les données collectées et traitées par les SSTI, qu'il s'agisse des données relatives aux entreprises adhérentes et de leurs salariés, des données concernant le personnel du Service, les documents et les informations produits ou encore la continuité de l'activité du Service, sont soumises réglementairement à des contraintes en termes de sécurité.

A ce sujet, la Commission Système d'Information (CSI) du Cisme a établi, avec la participation active d'un expert indépendant en sécurité des systèmes d'information de Santé, un document intitulé ***"Sécurité des systèmes d'information, ce qu'il faut savoir"***. En effet, il apparaît essentiel que les Services appréhendent les moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information.

Le Document a été rédigé à l'attention des Directions des SSTI, de leurs Conseils d'Administration, Commissions de Contrôle, ainsi qu'auprès des responsables des ressources humaines, informatiques, comptables, ou encore des médecins coordonnateurs et des Commissions Médico-Technique.

Après un rappel des principaux textes de loi relatifs à la sécurisation des données informatisées, il synthétise les actions à mettre en œuvre en fonction de leur caractère indispensable, nécessaire ou conseillé.

L'indispensable :

- **Faire les déclarations CNIL obligatoire**

Chaque traitement et/ou fichier contenant des données à caractère personnel doit être identifié et dûment déclaré auprès de la CNIL. Par exemple : le fichier du personnel des SSTI, le fichier des salariés suivis, le fichier des données médicales des salariés suivis, le fichier des entreprises adhérentes (s'il contient des données nominatives),…

- **Stocker les données de manière suffisamment sécurisée et séparée**

Les données personnelles à caractère médical ne peuvent être stockées sur les mêmes supports que les données administratives et les courriels. De plus, elles doivent avoir un niveau de sécurité suffisant. Ce stockage sécurisé doit être réalisé sur le serveur central, mais également sur les postes utilisateurs, ou encore sur les supports amovibles et dans les systèmes de messagerie.

- **Sauvegarder les données de manière régulière, vérifiée et sécurisée**

L'ensemble des données nécessaires au bon fonctionnement du Service doit être sauvegardé sur des supports amovibles et externalisés. La sauvegarde doit avoir une procédure rigoureuse permettant un retour en arrière. Il doit également être envisagé le stockage de ces sauvegardes, ainsi que la sécurité des données qui y sont inscrites. Enfin, ces sauvegardes doivent être testées régulièrement *"à blanc"*.

- **Gérer les droits d'accès de façon maîtrisée, notamment au niveau des habilitations d'accès aux données médicales**

Les accès aux lieux et aux données doivent être réglementés et compartimentés au *"besoin de voir et/ou d'agir "*. Des procédures strictes doivent être mises en place pour rendre inopérant tout accès inopiné d'un utilisateur ou d'un non-utilisateur à des espaces auxquels il n'aurait pas les droits. Enfin, l'ajout et le retrait d'utilisateurs doivent être correctement procédurés.

- **Rédiger une charte informatique**

Il convient d'avoir une charte informatique encadrant l'usage et le non-usage des outils technologiques au sein du Service.

Le nécessaire :

- **Mettre en œuvre une sauvegarde patrimoniale**

Les données médicales de suivi des salariés ont une durée maximale de conservation particulière, notamment dans le cas d'exposition à certains risques. Il convient de mettre en œuvre un processus particulier afin de répondre à ces exigences. Il est important de signaler que le processus de recouvrement ne répond pas aux mêmes besoins, il doit donc bien y avoir deux réflexions.

- **Gérer les codes malveillants (virus, hameçonnage,…)**

Les outils utilisés et installés doivent être opérants, c'est-à-dire qu'ils doivent être maintenus à jour de manière extrêmement précise. Ils doivent pouvoir être mis en arrêt par les utilisateurs. De plus, des cloisonnements de réseaux sont à mettre en œuvre afin de limiter une éventuelle défaillance des outils de protection.

- **Sécuriser et surveiller les communications**

Les communications entre sites, ou d'un site vers l'extérieur, doivent être sécurisées de manière adéquate au besoin (VPN [Virtual Private Network – Réseau privé virtuel en français] entre sites par exemple) et elles doivent faire l'objet d'une surveillance attentive afin de déceler toute intrusion ou comportement anormal.

- **Gérer et utiliser de manière sérieuse la traçabilité des accès**

L'ensemble des actions, et particulièrement les actions ayant un impact direct ou indirect sur les données personnelles à caractère médical, doivent être tracées, les traces doivent être stockées séparément. Ces traces doivent être vérifiées régulièrement afin d'identifier des actions inopportunes ou malveillantes.

- **Mettre en place un Plan de Continuité d'Activité (PCA) adapté et testé**

Un Service de santé au travail ne peut pas s'arrêter de fonctionner durablement, il convient donc de mettre en place un PCA conforme aux règles de l'art du moment. Ce PCA doit être régulièrement testé à blanc afin de ne pas être pris au dépourvu le cas échéant.