15 août 2010

GUIDE

Guide de bonnes pratiques de sécurisation du système d'information des cliniques

Sécurité sociale
L'Assurance Maladie

Synthèse du document

Ce guide de bonnes pratiques de sécurisation du système d'information est destiné aux cliniques dans le but d'améliorer la sécurité du système de facturation existant entre elles et l'Assurance Maladie.

Ce document se base sur la norme ISO 27 002 « Code de bonnes pratiques pour la gestion de la sécurité de l'information». Il en reprend les thématiques qui sont adaptées à la situation particulière du système de facturation des cliniques.

La CNAM-TS a pris en compte la maîtrise des risques concernant le système de facturation qui existent sur son réseau. Les cliniques doivent aussi maîtriser les risques au niveau de leur système d'information. En effet, en cas d'atteinte au système de facturation, leur responsabilité juridique et financière pourrait être engagée.

L'absence de précaution dans la sécurisation du système d'information peut conduire à mettre en danger la sécurité du système de facturation des cliniques, ce qui entraînerait un risque financier pour la clinique et/ou pour l'Assurance Maladie. Ce guide de bonnes pratiques est un ensemble de recommandations que les cliniques devraient appliquer à leur système d'information afin d'assurer la sécurité du système de facturation.

L'objectif des bonnes pratiques introduites dans ce guide est de :

- dissuader les éventuels attaquants,
- protéger au mieux le système de facturation contre les attaques,
- détecter les incidents et identifier leur origine.

Table des matières

1. Politique de sécurité

Les bonnes pratiques de sécurité recommandent la rédaction d'un document intitulé « Politique de Sécurité de l'Information » qui soit publié, visé par le management et communiqué à l'ensemble des employés et tiers. Ce document fournit, entre autre :

- Un cadre définissant la mise en place de contrôles au sein du système d'information et les objectifs de ces contrôles (entre autres permettre l'évaluation et de la gestion des risques).
- Une description succincte des directives, principes et standards de sécurité ainsi que des exigences de conformité qui méritent une attention particulière par rapport à l'organisation de l'entreprise.

	Recommandation
	■ Rédiger un document intitulé « Politique de Sécurité de l'Information et le communiquer à l'ensemble des employés et des tiers.

2. Gestion des biens

Le terme « biens » désigne l'ensemble du système d'information (matériel informatique, supports amovibles, applications logicielles,…) et des informations traitées (bases de données, traces d'audit,…).

Pour permettre une bonne maîtrise des risques il est souhaitable d'établir un inventaire des biens du système d'information. Une fois cet inventaire établi, il est alors possible de formuler les règles d'utilisation qui seront associées à chaque bien et qui devront être appliquées.

	Recommandations
	■ Établir un inventaire des biens du système d'information. ■ Documenter les règles d'utilisation ces biens ■ Appliquer ces règles d'utilisation

3. Sécurité liée aux ressources humaines

Pour limiter les risques portants sur le système d'information, il est souhaitable que tous les acteurs qui interviennent sur ce système soient conscients des risques.

Pour cela :

- Le management peut rappeler à tous les intervenants (employés, tiers…) qu'ils doivent appliquer les règles de sécurité en accord avec la politique et les procédures du système d'information.
- Ces mêmes intervenants devraient recevoir une formation de sensibilisation appropriée ainsi que des mises à niveau régulières sur les politiques et les procédures organisationnelles relatives à la sécurité dans l'exercice de leur métier.

	Recommandation
	■ S'assurer que l'ensemble des acteurs qui interviennent sur le système d'information (employés, contractants, tiers…) soient conscients des risques de sécurité existants et des mesures prises pour les limiter.

4. Sécurité physique et environnementale

Une bonne maîtrise des risques passe par la protection des accès physiques au système d'information :

- Au minimum aucun accès au système d'information ne devrait être possible depuis un emplacement accessible au public.
- Les éléments les plus sensibles du système d'information devraient aussi être plus particulièrement protégés (typiquement les serveurs devraient être installés dans une salle dédiée protégée par un contrôle d'accès ne permettant qu'aux personnes habilitées à y accéder)

	Recommandations
	■ Sécuriser physiquement l'accès aux zones contenant le système d'information. ■ N'autoriser l'accès à ces zones qu'aux seules personnes habilitées. En particulier ne pas permettre un accès au système d'information depuis un emplacement accessible au public.

5. Gestion de l'exploitation et des télécommunications

Les bonnes pratiques de sécurité recommandent la mise en œuvre de moyens conformes à l'état de l'art pour protéger les informations stockées ou en transit dans le système d'information.

Les moyens à mettre en œuvre consistent à protéger le système d'information des accès externes qui pourraient permettre la commission d'actes malveillants. Il s'agit aussi de sécuriser le transfert des informations sensibles au sein même du système d'information. Les informations doivent aussi être sauvegardées régulièrement.

	Recommandations
	■ Protéger le système d'information contre les accès malveillants. ■ Garantir l'intégrité et la confidentialité des échanges réalisés au sein du système d'information. ■ Mettre en place et documenter un mécanisme de sauvegarde des informations et logiciels du système d'information.

6. Gestion des droits d'accès

La maîtrise des risques est la gestion des droits d'accès accordés aux utilisateurs du système d'information, qu'il s'agisse d'employés ou de tiers. Il est important de pouvoir connaître à tout moment qui accède à quoi dans le système d'information.

Les utilisateurs ne doivent avoir les droits d'accès qu'aux seules parties du système nécessaire et ces accès doivent être donnés uniquement le temps nécessaire (et en particulier supprimés au départ de ces personnes). Une procédure formelle d'enregistrement et de désinscription des utilisateurs, destinée à accorder et à supprimer l'accès au système d'information, devrait être définie. Le mode opératoire d'enregistrement de l'utilisateur doit garantir que le niveau d'authentification de l'utilisateur soit cohérent avec le niveau d'accès autorisé par la suite (par exemple, une identification par face-à-face peut être requise pour certains accès sensibles).

Le contrôle d'accès peut être basé sur l'utilisation de rôles prédéfinis. Plusieurs rôles pouvant être attribués à un même utilisateur, et un rôle pouvant correspondre à une ou plusieurs fonctions.

	Recommandations
	■ Mettre en place une politique de contrôle d'accès au niveau du système d'information de la clinique basée sur des rôles. ■ Avoir une procédure claire d'enregistrement des utilisateurs au système d'information permettant d'accorder des droits d'accès sur le système, et de désinscription des utilisateurs du système d'information permettant de supprimer les droits d'accès existants sur le système. Contrôler l'identité des utilisateurs. ■ Réviser régulièrement les droits d'accès des utilisateurs. ■ Dans la mesure du possible, ne pas utiliser de compte générique et ne pas permettre à un utilisateur d'avoir plusieurs comptes. ■ Renforcer les moyens d'authentification pour l'accès au système d'information. Des mécanismes d'authentification forte (avec la carte CPS par exemple) seront préférés à l'utilisation de mots de passe. Si des mots de passe sont utilisés, une complexité minimale devrait être imposée ainsi qu'un renouvellement forcé sans réutilisation d'ancien mot de passe.

7. Acquisition, développement et maintenance des systèmes d'information

Une bonne pratique de sécurisation du système d'information est de le protéger constamment contre les vulnérabilités qui pourraient être découvertes.

Il est important pour cela de s'assurer dès l'achat d'un progiciel d'avoir le support nécessaire permettant d'avoir un correctif pour les vulnérabilités découvertes, et d'installer effectivement ces correctifs.

	Recommandations
	■ S'assurer dès le cahier des charges à l'origine du choix d'un progiciel de pouvoir disposer du support nécessaire à la correction des vulnérabilités majeures qui pourraient être découvertes. ■ Suivre la publication de correctifs de sécurité des progiciels utilisés et les installer.

8. Gestion des incidents de sécurité

Les incidents de sécurité survenant dans le système d'information doivent être traités avec la plus grande attention.

Les responsabilités et les procédures en termes de gestion des incidents devraient être établies en vue de :

- Garantir une réponse rapide, efficace et ordonnée aux incidents de sécurité.
- Garantir l'existence d'une communication efficace en matière d'incidents de telle sorte que les plans de gestion des crises et de continuité de l'activité puissent être invoqués en des circonstances appropriées et au bon moment.
- Regrouper et préserver les données relatives aux incidents telles que les traces d'audit, les journaux d'audit et autres preuves.

Les incidents de sécurité pourront être traités conjointement avec l'Assurance Maladie lorsque celle-ci est particulièrement concernée (par exemple s'il s'agit d'une atteinte au système de facturation).

	Recommandations
	■ Avoir une procédure en place permettant une réponse rapide, efficace et ordonnée aux incidents de sécurité du système d'information ■ Avertir via le correspondant RPS, l'Assurance Maladie lors de tout incident de sécurité qui pourrait la concerner. ■ Recenser l'ensemble des incidents qui impactent le système d'information et les analyser pour identifier les incidents de sécurité. ■ Conserver les preuves informatiques recueillies à la suite d'un incident de sécurité afin de pouvoir les utiliser dans le cadre d'une éventuelle action en justice. ■ Réviser la politique de sécurité après l'apparition d'un incident de sécurité important.