La sécurité informatique d'un centre d'imagerie médicale
Les conseils de la CNIL

Dr Hervé LECLET
Santopta

Tous les centres d'imagerie médicale doivent assurer la sécurité informatique de leur système d'information radiologique.
Pour cela, plusieurs actions doivent être mises en œuvre.
Ces actions sont détaillées dans le référentiel professionnel Labelix®.

2.5 La sécurité informatique du système d'information radiologique (SIR) (ou des fonctions SIR du système d'information) et du PACS est assurée par le site d'imagerie Dans les établissements de santé, le service d'imagerie n'est en général pas directement responsable de sa sécurité informatique. Il doit néanmoins s'assurer que celle-ci est respectée. Il doit également pouvoir en apporter la preuve.	**2.5.1 Un responsable de la sécurité du système d'information est nommé.** **2.5.2 La sécurité des accès aux logiciels métiers et aux données personnelles des patients est assurée par login et mot de passe individuel et par des déconnexions automatiques.** Les règles de renouvellement des logins et des mots de passe sont définies. **2.5 3 Les connexions sont tracées.** Il est possible d'accéder à l'historique des connexions par poste et par utilisateur. **2.5.4 Les échanges de données personnelles confidentielles sont sécurisés.** Par exemple : cryptage des données, pas d'envoi de comptes-rendus par simple mail, … **2.5.5 Les règles de sécurité des systèmes informatiques sont définies et mises en œuvre.** La synchronisation des données SIH / SIR / PACS est assurée et vérifiée selon une périodicité adaptée. Le réseau informatique et les postes de travail sont protégés par des onduleurs. La sécurité des réseaux Wifi est assurée par des clés d'accès. L'accès à Internet est sécurisé : • utilisation d'un firewall, • utilisation d'un antivirus avec mise à jour régulière, • … Le(s) serveur(s) est (sont) implanté(s) dans un endroit dédié, adapté et sécurisé. Un test de récupération des données est réalisé à périodicité définie **2.5.6 Une procédure écrite décrit l'organisation des sauvegardes.** Des sauvegardes sont réalisées régulièrement. Les archives informatiques sont gardées en dehors du site d'imagerie. On rappelle l'obligation réglementaire de sauvegarde des données du patient. **2.5.7 L'accès par l'extérieur au système informatique (pour réaliser des maintenances, pour travailler hors du cabinet/service) est protégé.** Par exemple par un login, un mot de passe, la définition des conditions d'accès. **2.5.8 Un plan de continuité de l'activité informatique est établi.** **2.5.9 Le site d'imagerie respecte la législation Informatique et Libertés.** Les traitements informatiques de données personnelles sont déclarés à la CNIL.

Cet article détaille les recommandations édictées par la CNIL en octobre 2009 dans le cadre du respect de la loi "Informatique et libertés".

La loi "Informatique et libertés" impose que les organismes qui mettent en œuvre des fichiers garantissent la sécurité des données qui y sont traitées. Cette exigence se traduit par un ensemble de mesures que les détenteurs de fichiers doivent appliquer, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique.

1. Adopter une politique de mot de passe rigoureuse

L'accès à un poste de travail informatique ou à un fichier par identifiant et mot de passe est la première des protections.
Le mot de passe doit être individuel, difficile à deviner et rester secret. Il ne doit donc être écrit sur aucun support.
La DSI ou le responsable informatique devra mettre en place une politique de gestion des mots de passe rigoureuse : un mot de passe doit comporter au minimum

8 caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment (par exemple tous les 3 mois).
Le système doit contraindre l'utilisateur à choisir un mot de passe différent des trois qu'il a utilisés précédemment.
Généralement attribué par l'administrateur du système, le mot de passe doit être modifié obligatoirement par l'utilisateur dès la première connexion. Enfin, les administrateurs des systèmes et du réseau doivent veiller à modifier les mots de passe qu'ils utilisent eux-mêmes.

2. Concevoir une procédure de création et de suppression des comptes utilisateurs

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non génériques (secrétaire1, secrétaire2, …), afin de pouvoir éventuellement être capable de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants.
En effet, les comptes génériques ne permettent pas d'identifier précisément une personne.
Cette règle doit également s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents chargés de l'exploitation du système d'information.

3. Sécuriser les postes de travail

Les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité (10 minutes maximum). Les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau.
Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application en cas d'absence momentanée de l'agent du poste concerné.
Par ailleurs, le contrôle de l'usage des ports USB sur les postes sensibles, interdisant par exemple la copie de l'ensemble des données contenues dans un fichier, est fortement recommandé.

4. Identifier précisément qui peut avoir accès aux fichiers

L'accès aux données personnelles traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées.
De cette analyse, dépend « le profil d'habilitation » de l'agent ou du salarié concerné.
Pour chaque mouvement ou nouvelle affectation d'un salarié à un poste, le supérieur hiérarchique doit identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès.
Une vérification périodique des profils des applications et des droits d'accès aux répertoires sur les serveurs est donc nécessaire afin de s'assurer de l'adéquation des droits offerts et de la réalité des fonctions occupées par chacun.

5. Veiller à la confidentialité des données vis-à-vis des prestataires

Les interventions des sous-traitants du système d'information doivent présenter les garanties suffisantes en termes de sécurité et de confidentialité à l'égard des données auxquels ceux-ci peuvent, le cas échéant, avoir accès.
La loi impose ainsi qu'une clause de confidentialité soit prévue dans les contrats de sous-traitance.

Les éventuelles interventions d'un prestataire sur des bases de données doivent se dérouler en présence d'un salarié du service informatique et être consignées dans un registre.
Les données qui peuvent être considérées « sensibles » au regard de la loi, par exemple des données de santé ou des données relatives à des moyens de paiement, doivent au surplus faire l'objet d'un chiffrement.

A noter : l'administrateur systèmes et réseau n'est pas forcément habilité à accéder à l'ensemble des données de l'organisme. Pourtant, il a besoin d'accéder aux plates-formes ou aux bases de données pour les administrer et les maintenir. En chiffrant les données avec une clé dont il n'a pas connaissance, et qui est détenue par une personne qui n'a pas accès à ces données (le responsable de la sécurité par exemple), l'administrateur peut mener à bien ses missions et la confidentialité est respectée.

6. Sécuriser le réseau local

Un système d'information doit être sécurisé vis-à-vis des attaques extérieures.
Un premier niveau de protection doit être assuré par des dispositifs de sécurité logique spécifiques tels que des routeurs filtrants (ACL), pare-feu, sonde anti intrusions, etc. Une protection fiable contre les virus et logiciels espions suppose une veille constante pour mettre à jour ces outils, tant sur le serveur que sur les postes des agents.
La messagerie électronique doit évidemment faire l'objet d'une vigilance particulière.
Les connexions entre les sites parfois distants d'une entreprise d'imagerie doivent s'effectuer de manière sécurisée, par l'intermédiaire des liaisons privées ou des canaux sécurisés par technique de « tunneling » ou VPN (réseau privé virtuel).
Il est également indispensable de sécuriser les réseaux sans fil (wifi) compte tenu de la possibilité d'intercepter à distance les informations qui y circulent : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés, etc.
Enfin, les accès distants au système d'information par les postes nomades doivent faire préalablement l'objet d'une authentification de l'utilisateur et du poste. Les accès par internet aux outils d'administration électronique nécessitent également des mesures de sécurité fortes, notamment par l'utilisation de protocoles IPsec, SSL/TLS ou encore HTTPS.

7. Sécuriser l'accès physique aux locaux

L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités. Ces locaux doivent faire l'objet d'une sécurisation particulière : vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc.
La DSI ou le responsable informatique doit veiller à ce que les documentations techniques, plans d'adressages réseau, contrats, etc. soient eux aussi protégés.

8. Anticiper le risque de perte ou de divulgation des données

La perte ou la divulgation de données peut avoir plusieurs origines : erreur ou malveillance d'un salarié ou d'un agent, vol d'un ordinateur portable, panne matérielle, ou encore conséquence d'un dégât des eaux ou d'un incendie.

Il faut veiller à stocker les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières. Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs, idéalement dans un coffre ignifugé.
Les serveurs hébergeant des données sensibles ou capitales pour l'activité doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne. Il est recommandé d'écrire une procédure « urgence – secours » qui décrira comment remonter rapidement ces serveurs en cas de panne ou de sinistre majeur.
Les supports nomades (ordinateurs portables, clé USB, assistants personnels, etc.) doivent faire l'objet d'une sécurisation particulière, par chiffrement, au regard de la sensibilité des dossiers ou documents qu'ils peuvent stocker.
Les matériels informatiques en fin de vie, tels que les ordinateurs ou les copieurs, doivent être physiquement détruits avant d'être jetés, ou expurgés de leurs disques durs avant d'être donnés à des associations. Les disques durs et les périphériques de stockage amovibles en réparation, réaffectés ou recyclés, doivent faire l'objet au préalable d'un formatage de bas niveau destiné à effacer les données qui peuvent y être stockées.

9. Anticiper et formaliser une politique de sécurité du système d'information

L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des agents ou des salariés.
Sa rédaction requiert l'inventaire préalable des éventuelles menaces et vulnérabilités qui pèsent sur le système d'information.
Il convient de faire évoluer régulièrement ce document, au regard des modifications des systèmes et outils informatiques utilisés par l'entreprise d'imagerie.
Enfin, le paramètre « sécurité » doit être pris en compte en amont de tout projet lié au système d'information.

10. Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "Informatique et libertés"

Le principal risque en matière de sécurité informatique est l'erreur humaine.
Les utilisateurs du système d'information doivent donc être particulièrement sensibilisés aux risques informatiques liés à l'utilisation de bases de données. Cette sensibilisation peut prendre la forme de formations, de diffusion de notes de service, ou de l'envoi périodique de fiches pratiques.
Elle sera également formalisée dans un document, de type « charte informatique », qui pourra préciser les règles à respecter en matière de sécurité informatique, mais aussi celles relatives au bon usage de la téléphonie, de la messagerie électronique ou encore d'internet. Ce document devrait également rappeler les conditions dans lesquelles un salarié ou un agent peut créer un fichier contenant des données personnelles, par exemple après avoir obtenu l'accord de son responsable.
Ce document doit s'accompagner d'un engagement de responsabilité à signer par chaque utilisateur.
A noter : veiller à ce que les utilisateurs nettoient régulièrement leurs vieux documents et messages électroniques sur leurs postes.
De même, nettoyer régulièrement le répertoire d'échange partagé entre les différent services afin qu'il ne se transforme pas en espace « fourre-tout » (fichiers personnels des agents mélangés avec des dossiers sensibles).

En pratique
Pour sécuriser les données de santé dans les applications en réseau

La gestion des mots de passe
- Code utilisateur individuel distinct du nom de l'utilisateur.
- Interdiction de réutiliser les trois derniers mots de passe (blocage du système).

Modalités de connexion et de déconnexion
- Impossibilité pour les utilisateurs de se connecter à plusieurs sous le même code utilisateur et le même mot de passe.
- Indication systématique aux utilisateurs lors de la connexion, sous forme d'un affichage sur l'écran, des dates et heures de la dernière connexion sous les mêmes code utilisateur et mot de passe.

Journalisation des connexions et exploitation de ces données
- Après plusieurs frappes (ex. trois) incorrectes successives du mot de passe (associé à un code utilisateur correct), blocage de l'accès et message demandant à l'utilisateur d'appeler le responsable du système.
- Procédure de déconnexion automatique en cas de non-utilisation du système pendant un temps donné (time out).
- Utilisation dans la mesure du possible de cartes à puce ou dispositifs analogues.

La confidentialité des données
- Utilisation dans la mesure du possible du codage des données nominatives.
- Cryptage de tout ou partie des données dans le cadre de la réglementation française et européenne en vigueur**.**

L'intégrité des données
- Mise en place de protocoles de transmission adaptés permettant de vérifier la conformité des données reçues à celles émises.
- Lors de la numérisation et de la compression des images (imagerie médicale), utilisation de procédures normalisées permettent de garantir l'intégrité de ces données.

En cas d'architecture client-serveur
- Prendre les dispositions nécessaires pour gérer le rapatriement des données ou le transfert de fichiers sur micro-ordinateur en fonction des habilitations de chacun : limitation au minimum du transfert de fichiers complets, limitation du volume des informations rapatriées, journalisation des requêtes au niveau du serveur.
- Restriction d'accès aux données en fonction des habilitations.
- Séparation des réseaux de gestion administrative et de suivi médical.

Connexion à Internet
- En cas de connexion d'un des serveurs du réseau à Internet, prévoir des mesures de sécurités particulières comme la séparation physique des deux réseaux, la mise en place d'un firewall ou de barrières de protection logicielles.
- Lorsque des données de santé sont transférées via Internet, recourir au chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits).