LA PROTECTION DU SECRET MÉDICAL : RETOUR D'EXPÉRIENCE SUR LE CONTRÔLE DES ACCÈS AU DPI

Par Bertrand LEBIN, Dirigeant de DAQSAN

1. La problématique du contrôle des accès

Le logiciel de gestion du DPI est au cœur de l'activité des établissements de santé. Historiquement ce dossier médical était enregistré sous forme papier, et consultable au sein d'archives. Aujourd'hui il est numérisé et accessible via toute connexion interne. Cette évolution des usages a facilité le côté opérationnel mais a complexifié la gestion de ses accès et ceci pour plusieurs raisons :

D'abord parce que la taille des établissements de santé peut être très importante (nombre de lits, nombre de services, nombre d'agents, etc.). Leurs effectifs sont conséquents, avec de surcroît une forte mobilité interne. De ce fait, vouloir paramétrer au quotidien les droits régissant le contrôle des accès et dresser une cartographie précise de la situation des agents tient de l'utopie. Il est donc fréquent de constater un décalage entre les informations connues au niveau RH et la réalité du terrain.

Ensuite parce que la réponse en termes de protection se limite à deux options :

• La fermeture stricte des accès à tout le personnel non concerné, avec comme avantage de renforcer la protection. Mais cela limite les professionnels qui ne peuvent plus accéder aux dossiers en cas d'urgence.

• Une ouverture des droits plus permissive, avec parfois l'utilisation de la fonction bris de glace qui permet de consulter n'importe quel dossier.

Pour favoriser une prise de connaissance rapide du dossier du patient, c'est aujourd'hui cette option qui est privilégiée avec comme conséquence un risque sur la confidentialité et sur la sécurité des données.

Et enfin parce qu'elle doit satisfaire deux besoins majeurs :

• Respecter les contraintes réglementaires en répondant de manière adaptée à la problématique du RGPD sur la protection des données sensibles.

• Protéger le secret médical dans un contexte de cas avérés de curiosité déplacée, d'absence de sensibilisation sur le sujet, et d'intrusions volontaires ciblées.

2. Notre retour d'expérience

Le point de départ de cette aventure a été la rencontre avec le directeur informatique d'un établissement de santé qui m'a présenté cette problématique. Notre expertise en data management, concrétisée au travers de projets importants dans le domaine des banques et des assurances sur de gros volumes d'informations sécurisées, a fait écho à son besoin. À partir de là, il était clair que cette expérience acquise pouvait être transposée au monde médical.

Après quelques séances collaboratives, ce directeur a exposé son inquiétude face à la capacité de détecter des comportements utilisateurs complexes sur des grands volumes d'informations grâce aux traces fonctionnelles des actes médicaux. Il précisa certaines contraintes telles que : les traces médicales restent en interne, la détection des usages suspects doit être paramétrable.
Pour illustrer son propos il nous challengea sur un cas difficile à détecter :

1. L'utilisateur crée un rendez-vous.
2. Il accède au dossier d'un patient.
3. Le patient correspond à un agent de l'établissement.
4. L'utilisateur annule le rendez-vous.
5. Tout cela dans un délai très court.

En pratique, cela revient à rechercher un triplet de traces fonctionnelles successives A, B, C, possédant chacune des caractéristiques spécifiques et correspondant au même couple (agent, patient), avec de surcroît la possibilité que le patient soit aussi un agent de l'établissement de santé.

Il a été nécessaire d'analyser les logs fonctionnels pour trouver les traces pertinentes, les croiser avec la base des Ressources Humaines. Compte tenu de la volumétrie il n'a pas été possible manuellement d'y répondre. Je lui ai proposé d'adapter une solution interne de Data Management pour tenter d'obtenir le résultat souhaité. Le test réalisé au sein de son système d'information a été concluant et a permis la détection des cas souhaités.

Par la suite, avec les équipes du DIM, nous avons identifié un ensemble de règles de détection à mettre en œuvre et coconstruit un workflow permettant l'instruction des dossiers trouvés. En termes de résultats, la méthode la plus adaptée fût de :

1. Mettre une routine de contrôle, à postériori basée sur des détections d'abus, en utilisant une solution logicielle croisant les logs de consultations avec la base RH.
2. Sensibiliser le personnel en interne, par un accompagnement pédagogique.
3. Instruire les cas suspects détectés en suivant une démarche interrogative.

Ce fut la première fois, depuis les différentes campagnes d'informations et de préventions, que des agents ont dû répondre à des demandes d'explications sur la base de faits avérés. Cette exigence de transparence a généré une prise de conscience globale avec comme conséquence une diminution des usages suspects.

Force est de constater que depuis ces tests, un climat de respect et de bienveillance s'est installé au sein de cet établissement de santé de plus de trois mille agents. Et concrètement, dès la première année, il a été constaté une diminution de plus de 50% des cas suspects.

Mois	Ano critiques	Diminution	Logs analysés
Février	**48**		**1,9 M**
Juin	**24**	**50%**	**2,0 M**
Novembre	**20**	**58%**	**1,9 M**

Désormais, un seuil minimal de cas suspects semble avoir été atteint. Il est régulièrement perturbé par des évènements de natures diverses : arrivée de nouveaux personnels, épidémie, faits divers, etc…
Depuis, le RSI nous a challengé sur la détection des actes médicaux non facturés à tort, en croisant les actes des applications métiers avec la GAM. A nouveau les résultats sont là ! L'établissement facture des actes précédemment rejetés, automatise la justification de ses écarts pour les commissaires aux comptes. Le ROI est prometteur :

• Récupération de recettes sur actes précédemment non facturés

• Gain de temps sur les activités fastidieuses de justification des comptes...

3. Pour aller plus loin

La solution DPI Protect permet de :

• Lancer une analyse quotidienne de 100 % des traces fonctionnelles du DPI croisées avec les éléments de la base des Ressources Humaines.

• Utiliser un catalogue de règles de détection des usages suspects, paramétrable et adapté à chaque établissement.

• Pouvoir se connecter aux différentes solutions DPI et RH.

En termes de réponse notre solution :

• Favorise le changement de comportement des agents par une confiance retrouvée suite à un processus d'accompagnement.

• Met en évidence la preuve RGPD de la diminution des cas constatés et la nécessité de l'engagement de la direction sur ce sujet.

RECETTE DAQSAN

La bonne recette de l'auteur pour la mise en place de la protection du DPI

1. Je récupère l'information de sources diverses
2. Je la méta-modélise pour la rendre exploitable
3. Je la transforme et l'enrichis
4. Je croise mes traces fonctionnelles et ma base RH
5. Je paramètre mes alertes
6. J'exécute ma détection de cas
7. J'instruis et classe mes résultats
8. J'automatise ce qui peut l'être

DAQSAN
www.daqsan.fr
commercial@daqsan.fr
02.51.05.28.68