OPUS 3

APSSIS

GUIDE CYBER RÉSILIENCE

LES HABILITATIONS D'ACCÈS AUX DONNÉES

À PROPOS DU DROIT D'EN CONNAÎTRE

SOMMAIRE

CYBER RÉSILIENCE

0.3 LES HABILITATIONS D'ACCÈS AUX DONNÉES

SOMMAIRE

CYBER RÉSILIENCE

0.3

1. INTRODUCTION

Informatiser un processus métier revient, stricto sensu, à automatiser le traitement des données, ce qui conduit à traiter plus de données, plus vite, pour le bénéfice de plus de clients / usagers, et accessibles à plus de monde en interne / externe.

Or, quand les données des établissements n'étaient physiquement disponibles que sous un format papier, à de rares exceptions, les fuites et les problématiques d'accès (qui peut voir quoi, qui peut modifier quoi) étaient quasi inexistantes. Avec l'informatisation et surtout l'interconnexion des réseaux (le Web entre autres), la question de l'accès devient plus prégnante.

Que dans une PME de 10 personnes, tout le monde ait accès aux données client (la GRC, Gestion de la Relation Commerciale) ne choquera personne : après tout, il faut bien faire tourner l'établissement. Que dans cette même PME, tous les employés aient accès aux données RH de tout le monde posera plus de problèmes : il s'agit de données sensibles, et l'employé X n'a aucune légitimité à connaître la situation familiale, fiscale (taux de retenue à la source), professionnelle (salaire, prime, appréciation de la hiérarchie, etc.) de l'employé Y sauf si X est responsable du processus RH.

Immanquablement, l'informatisation de données métier (comptables, RH, facturation, cœur de métier, etc.) est indissociable de la question des habilitations d'accès à ces mêmes données. Selon que l'établissement compte 10 ou 10 000 salariés, selon qu'elle évolue dans un domaine fortement réglementé ou pas, selon la nature des données traitées, les réponses ne sont pas les mêmes.
Ce guide a pour objectif de poser clairement le problème, de présenter les différentes approches possibles avec leurs avantages et inconvénients, de sensibiliser le lecteur aux questions connexes de telle sorte à disposer d'une vision globale du sujet. Il s'adresse aussi bien aux professionnels de santé qu'aux décideurs ou aux DSI.
Une précaution s'impose toutefois : le sujet des habilitations d'accès aux données de santé est complexe et a connu de gros changements depuis les premières générations de DPI au début des années 2000.

Sur certaines questions de fond, les réponses sont connues, classées, rangées. Sur d'autres questions, il n'y a pour le moment que des avis, susceptibles d'évolution dans les prochaines années. Et sur certaines questions enfin, les spécialistes des différents métiers (corps médical, corps soignants, DSI, juristes, RSSI, etc.) ne sont pas même pas d'accord sur la formulation de la question. Ce guide doit donc n'être pris que pour ce qu'il est : une tentative de poser les bases et les problèmes, de décrire l'état des connaissances et du débat sur la question, et certainement pas de proposer LA solution urbi et orbi à l'ensemble des questions. Ecrit il y a 10 ans, ce guide n'aurait certainement pas eu la même teneur, écrit dans 10 ans non plus.

Les contributions en annexes constituent un témoignage précieux de la vision de professions différentes : directrice, médecin, éditeur, etc. Que ces visions ne soient pas toutes alignées, qu'elles abordent le sujet par différents angles d'attaques, qu'elles ne posent pas les mêmes questions et ne proposent pas les mêmes pistes de solutions est exactement l'objectif du présent guide.

Après le premier guide « Cyber résilience - les mots de passe » et le deuxième guide « Cyber résilience - les cyber attaques », ce troisième opus poursuit la réflexion globale autour de la sécurité des SIH. Et comme toujours, les remarques, suggestions d'amélioration sont à envoyer directement à l'auteur pour être prises en compte dans les prochaines versions.

Bonne lecture.

L'AUTEUR

Cédric CARTAU est RSSI et DPO du CHU de NANTES et du GHT44. Il est vice-président de l'APSSIS et enseigne à l'EHESP, à l'ESIEA et au CNEH. Il est également auteur de plusieurs ouvrages chez Eyrolles ou aux Presses de l'EHESP, sa dernière publication étant « La sécurité du système d'information des établissements de santé », en 2018.

cedric@cartau.net

Ont participé à la rédaction de ce guide les personnes suivantes par ordre alphabétique :

M° François COUPEZ, Avocat
Loïc GUEZO, PROOFPOINT
Dr Pierre LAFAY, Ancien Président de CME du CH de DAUMEZON
Bertrand LEBIN, DAQSAN
Romain LE GUILCHER, Nadou YEO et Lân GUICHOT, EVOLUCARE
Dr Nicolas MAUDUIT, Médecin DIM du CHU de NANTES
Anne-Sophie MAURE DE LIMA, Directrice des Usagers, des Services aux Patients et des Partenariats Innovants du CHU de NANTES

L'auteur et l'APSSIS remercient ces contributeurs d'avoir accepté le difficile exercice de présenter une approche métier sur une question aussi complexe que l'accès à la donnée en général, et à la donnée médicale en particulier.

proofpoint.

DAQSAN
PROTECTION • SÉCURITÉ • VALORISATION

evolucare

APSSIS

2. Les fondamentaux

2.1 Les réglementations opposables

Les réglementations relatives au droit d'en connaître - ce qui est l'expression consacrée - des données métier sont de trois natures :

• **les réglementations généralistes** : il y a bien évidemment le RGPD, mais aussi une partie du corpus législatif existant dans le Code du travail, le Code Pénal, etc. ;

• **les réglementations sectorielles** : dans la santé, il s'agit du Code de la Santé Publique (CSP) ;

• **le corpus normatif** qui, sans relever forcément du niveau de la loi, s'impose pour autant : on pense par exemple à la certification ISO 15189 qui s'impose aux pôles de Biologie, à la Certification des Comptes qui traite de la sécurisation des flux financier, etc. ;

La certification ISO 27001 et la question des habilitations

Lorsqu'une DSI s'engage dans une certification ISO 27001, elle devra à un moment donné régler la question des habilitations d'accès de ses personnels inclus au périmètre de certification, aux données et aux outils métiers également inclus dans ce périmètre : logiciels d'administration, accès admin, etc.

Même si ce ne sont pas stricto sensu des accès à des données métier telles des données médicales ou RH, le principe et le sujet sont exactement ceux décrits dans ce présent opus.

2.2 Les niveaux de classification des données

Il est courant de classer les données en quatre familles, selon leur niveau de « sensibilité » au critère de confidentialité. Nous emploierons les termes suivants :

• **niveau PUBLIC** : la donnée peut être connue de toute personne, aussi bien interne qu'externe à l'établissement ; par exemple le nombre d'agents, le numéro SIRET, etc. ;

• **niveau INTERNE** : la donnée peut être connue de toute personne en interne de l'établissement, mais n'a pas à être divulguée à l'extérieur de celle-ci ; par exemple la marque du Firewall (impact sur la sécurité informatique) ou tel rapport interne sur les fiches d'événements indésirables ;

• **niveau RESTREINT** : la donnée n'est consultable qu'en interne et que par une catégorie d'individus ; par exemple les données financières uniquement par les agents du pôle finance, les données RH uniquement par les agents de la DRH, etc. ;

• **niveau CONFIDENTIEL** : la donnée n'est consultable que par une liste d'individus nommés ; à la différence du niveau RESTREINT où l'on parle d'une catégorie d'individus, là il s'agit d'une liste fixe

comportant les noms et prénoms des seules personnes ayant intuitu personæ accès à la donnée ; par exemple les données de médecine du travail des agents de l'établissement (données ultra sensibles accessibles uniquement par la liste des agents du service de médecine du travail), les mots de passe admin de domaine de l'Active Directory, etc. ;

Le cas des prestataires

Qu'une personne soit prestataire sous contrat n'est pas incompatible avec le fait que cette même personne ait accès à des données de niveau RESTREINT, ou CONFIDENTIEL. Il s'agira de la positionner dans les bons groupes, et de veiller à l'existence de clauses contractuelles adéquates.

2.3 Opposition DIC

2.3.1 Généralités

Toute la sécurité SI s'articule autour de quatre concepts : DICP. D pour Disponibilité, I pour Intégrité, C pour Confidentialité et P pour Preuve (ou traces). Le dernier critère (P) n'est pas pertinent pour ce guide, seuls nous intéressent pour le moment DIC.

La Disponibilité est la capacité d'un système à fonctionner. Quand votre voiture est en panne, il s'agit d'un accident de disponibilité. Idem lorsque le DPI plante pendant 4h.

L'Intégrité est la capacité d'un système à garantir qu'une donnée n'est pas altérée, que ce soit par une action technique (bug) ou humaine, volontaire ou pas. Si votre feuille d'impôts comporte une erreur, il s'agit d'un accident d'intégrité. Idem si le poids sur la fiche d'un patient est accidentellement divisé par 100.

La Confidentialité, objet de ce présent guide, est la capacité d'un système à garantir que seules les personnes « ayant besoin d'en connaître » ont réellement accès à une donnée. Si votre voisin de palier reçoit par La Poste votre feuille d'impôts à votre place, il s'agit d'un accident de confidentialité. Idem si le dossier médical d'un chanteur connu fuite dans la presse.

2.3.2 Nécessaire arbitrage

Le côté complexe de cette séparation est qu'il s'agit d'un compromis : toute surpondération d'un des trois critères se fait forcément au détriment d'un des deux autres. C'est une loi générale contre laquelle on ne peut rien.

Par exemple, le dossier médical (DM) le plus disponible du monde (surpondération du D) est celui qui est dans Google (altération du C). Inversement, le DM le plus confidentiel du monde (surpondération du C) est celui que l'on détruit physiquement (altération du D et du I). Dans les faits, l'arbitrage se fait essentiellement entre le D et le C, le I est moins impacté dans cette danse à trois.

Au regard de la sécurité du SI, tout système est donc un compromis entre ces trois critères. Il n'existe pas de choix parfait et

unique. Il s'agit d'une question qui se pose à chaque déploiement de progiciel et qui est secteur-dépendant, métier-dépendant, époque-dépendante, etc. Les choix DIC ne seront pas les mêmes selon qu'il s'agisse d'un progiciel RH, des Urgences d'un CHU, du DPI d'un établissement psychiatrique, d'un service de médecine interne, etc. Et la vision de cette articulation - de ce compromis nécessaire - a fortement évolué dans le temps comme nous le verrons plus loin.

DIC et RGPD

Une erreur fréquemment commise est celle qui consiste à penser que le RGPD (et les réglementations Informatiques et Libertés précédentes) ne se préoccupent que de la confidentialité des données personnelles. C'est faux : la réglementation précise bien que la sécurité des données est à aborder au sens large dans ces trois dimensions DIC. Dans le texte :

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Le sujet devient singulièrement complexe dès lors que l'on « mixe » des activités ayant des objectifs antagonistes : un DPI commun à des activités d'urgences, de chirurgie, de MCO, de psychiatrie, de médico-social, etc., doit-il privilégier le D ou le C ?

ÉVALUER LA SENSIBILITÉ DE DONNÉES PERSONNELLES, ET NOTAMMENT DES DONNÉES DE SANTÉ : ANALYSE MICRO OU MACRO ? LA VISION DE L'AVOCAT

Par Maître François COUPEZ, Avocat associé du Cabinet Implid Legal, (ex ATIPIC Avocat), Titulaire du certificat de spécialisation en droit des nouvelles technologies (CNB) et de la certification DPO agréée par la CNIL.

1. Notions de « données de santé »

La notion de « données de santé » a évolué depuis le RGPD. Notion auparavant non définie en tant que telle, les « données relatives à la santé » mentionnées dans la directive 1995/46 ont évolué pour devenir des « données concernant la santé » dans le RGPD. L'article 4. 15) de ce texte les définit comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ».

A lire le considérant 35 du même texte, la notion est très large et intègre entre autres[1] « *toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro* ».

Ces données, en plus d'être considérées comme des « catégories particulières de données à caractère personnel » (article 9) et qui sont donc interdites de traitement par principe, voient leur protection renforcée par le même article *in fine*[2] . Cette disposition donne en effet la possibilité aux États membres de maintenir ou introduire des conditions supplémentaires, y compris des limitations pour leur traitement, ce que le législateur français a fait avec les articles 64 à 77 de la loi Informatique et libertés du 6 janvier 1978 pour un certain nombre de traitements de données de santé[3].

Toutefois, quelle que soit la catégorisation des données personnelles et la façon dont elles doivent être considérées au regard du

1 Sont également comprises « des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (9) au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; (…) ».

2 Ainsi que l'article 36 in fine.

3 Via la loi 2018-493 du 20 juin 2018 - cf. art. 53 et suivants de la loi dans sa version d'alors, plusieurs fois modifiée depuis.

droit applicable, la question de l'évaluation réelle de la sensibilité d'une donnée personnelle se pose toujours. Elle s'avère en réalité toujours difficile à appréhender *a priori* et explique que les exigences du RGPD comme de la directive 1995/46 qui l'a précédé ou de la loi de 1978 avant eux en France se focalisent sur la notion d'évaluation des risques et de protection des données au regard des risques supposés, le terme même de « risque » étant répété à 78 reprises dans le RGPD.

2. L'évaluation des risques… en théorie

Le principe, cardinal, est mentionné dès l'article 5. f) où sont rappelées les idées de « *sécurité appropriée* » ou encore de «*mesures techniques ou organisationnelles appropriées* ». Il est repris notamment par la suite aux articles 25 (Protection des données dès la conception et protection des données par défaut) et 32 (Sécurité du traitement)[4].

Surtout, dès l'article 24, le responsable du traitement se voit spécifiquement confier le soin d'évaluer les risques et de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD. Le texte précise également que « *Ces mesures sont réexaminées et actualisées si nécessaire* ».

Derrière ces notions apparaît ainsi non seulement la valeur objective, *erga omnes*, de la donnée, mais également l'appréciation de la valeur subjective pour certains tiers comme pour la personne concernée par cette donnée, valeur qui dépend de situations possiblement très différentes. C'est justement sur cette perception par des tiers de la valeur d'une donnée, et donc de l'appréciation complexe du risque de sa perte de confidentialité, que nous nous concentrerons ici.
Rappelons en effet que la valeur éventuellement patrimoniale de ces informations peut expliquer l'intérêt que des pirates pourraient avoir pour celles-ci et donc le niveau de risque réel pour l'entreprise ou les établissements la détenant.

Prenons ainsi un exemple *a priori* facile : un célèbre joueur de football se blesse dans sa vie privée.
Cette même information concernant sa blessure est notamment de nature à :

• lui faire perdre une valeur patrimoniale importante pour son club qui envisageait justement de le « revendre » avec bénéfice au prochain *mercato* ;

• fausser la cote des parieurs sur le prochain match auquel il est censé participer ;

• servir à alimenter les traitements big data d'une équipe nationale concurrente qui en déduira, lors de la prochaine Coupe du

4 Article 32 : « *1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées (…)* ».

monde, ses potentiels points de fragilité.

Jusque-là rien de bien nouveau : les risques sont connus, donc identifiables, et les équipes sportives professionnelles ont très souvent leur propre équipe médicale dédiée permettant de cantonner l'information, se rajoutant au secret médical auquel les membres de l'équipe soignante sont tenus de façon générale.

Prenons donc un cas plus complexe… et plus actuel : le fait qu'un salarié soit ou non porteur de la COVID-19. La situation des mois passés montre que l'employeur a été amené et le sera sans doute encore, souvent indirectement et à son corps défendant, à connaître cette information, indubitablement médicale, voire à la traiter (pour organiser l'information des cas contacts au sein de l'entreprise, gérer l'isolement, etc.).

Si la situation d'urgence sanitaire peut expliquer, à défaut de légitimer, le fait que les employeurs soient amenés à connaître plus que nécessaire la santé de leur salarié, les risques d'abus sont nombreux. Et si le salarié est soupçonné d'être venu travailler et d'être à l'origine d'un cas de « super propagation » dans l'entreprise, ayant conduit de surcroît, à des cas graves voire des décès ? La preuve de la date à laquelle il s'est fait tester, et surtout a obtenu les résultats et l'action qu'il a pu entreprendre auprès de l'entreprise à partir de là, vont s'avérer cruciales.

L'employeur qui s'efforcera de respecter les règles et de ne pas traiter la donnée de santé correspondant à la contamination ou pas par cette maladie, risque d'être dépassé en pratique par les inférences que pourraient faire les autres salariés à partir de certains faits particuliers objectifs.

3. L'évaluation des risques… en pratique

Dans ce cadre, il est essentiel de prendre en compte des scénarios intégrant non seulement la valeur de sa donnée personnelle pour la personne concernée, mais également pour des tiers qui, en fonction des circonstances, pourraient en tirer profit. De façon plus complexe, il apparaît de plus en plus nécessaire d'étendre la protection à des informations qui, sans être des informations de santé en elle-même, peuvent facilement faire deviner la réalité de ces données - ce qu'on appelle fréquemment « des données de santé par inférence ».

Ainsi, imaginons qu'une plateforme de réservation de rendez-vous médicaux considère qu'elle ne traite pas de données de santé, ne s'occupant que de la gestion administrative des rendez-vous pris. La fréquence des rendez-vous, d'une part, et la spécialité des praticiens, d'autre part, permettront d'inférer des informations quant à la santé, physique ou mentale, des utilisateurs de la plateforme. Cela est d'autant plus vrai si l'on croise ces données avec la fréquence de consultation de spécialistes d'une même spécialité ou de la recherche de profils très particuliers sur le moteur de recherche de la plateforme.

Vous avez consulté quatre cancérologues différents et vous consultez régulièrement depuis un chirurgien urologue ? Vous

recherchez depuis peu un spécialiste de la « *rééducation après cancer du rein* » ? Deviner la pathologie dont vous souffrez devient un jeu d'enfant. D'ailleurs, le type de rééducation proposé ici est l'intitulé, au mot près, qu'une plateforme de réservation a pu proposer à l'auteur de cet article lors des recherches préalables à la rédaction de cet article !

Cet exemple démontre bien qu'à l'occasion d'un traitement de données personnelles, toutes les fonctionnalités offertes aux utilisateurs sont donc à scruter (l'intelligence artificielle du moteur de recherche, les champs ouverts aux commentaires complémentaires des internautes, etc.) au regard des données, notamment de santé (par inférence ou non), qu'elles conduisent in fine l'utilisateur à indiquer.

Au-delà de la protection de personnes connues, médiatiquement ou politiquement exposées, auxquels les organismes de soin ont souvent prévu une protection complémentaire au « simple » respect du secret médical (inscription ou pseudonyme, statut « VIP », etc.), les nouvelles technologies, et en particulier l'intermédiation poussée qu'elles rendent possible, interrogent aujourd'hui sur la protection renforcée du simple *quidam*.

Les hypothèses se multiplient où la valeur subjective des informations augmente en parallèle de la croissance des vecteurs de l'exploitation financière de cette donnée. En outre, ce ne sont plus seulement les données personnelles qui sont concernées, mais également les données anonymisées : en tant qu'assureur, ne serait-il pas intéressant que je traite les données *open data* de consultation des spécialistes d'une pathologie particulière sur un territoire géographique donné afin que je croise par exemple ces données avec les facteurs d'origine ou de risque de cette pathologie et que j'en tire toutes les conséquences sur les primes d'assurance des clients de ce territoire ?

Quelles conséquences pratiques en tirer ? La notion de donnée appartenant à une « *catégorie particulière de données à caractère personnel* » est à géométrie variable et son analyse ne doit pas se cantonner à sa définition juridique, quelque peu réductrice, mais bien s'adosser à une analyse extra juridique. La réalité est complexe et l'appréhension de la sensibilité doit aussi être vue au travers du prisme de la valeur de la donnée, appréciée objectivement, mais aussi subjectivement par la personne concernée et plus largement par d'autres personnes, parties prenantes intéressées par cette donnée. Cette valorisation de la donnée a pour conséquence d'enrichir l'analyse du risque relatif à cette donnée et doit conduire à une approche plus réaliste de celui-ci.

Plus que jamais les analyses de risque, qu'elles soient réalisées comme des analyses d'impact relative à la protection des données (AIPD) ou de façon plus synthétique, doivent intégrer les scénarios les plus divers et associer, pour leur élaboration, des profils variés permettant de mieux appréhender la réalité des risques actuels.

Enfin, elles doivent être documentées afin de conserver l'historique non seulement des décisions prises, mais encore des diligences accomplies, des arbitrages réalisés et des raisons qui les sous-tendent.

3. ELÉMENTS D'APPROCHE

La question du droit d'en connaître dans les progiciels métier se divise en deux :

• quelles sont les identités utilisateurs (ID) qu'il faut créer, et comment : à partir de quelle source de données, avec quel outil ou processus, etc. ;

• pour ces ID, quelles habilitations faut-il attribuer : à partir de quel modèle général, à partir de quelles informations, avec quel outil ou processus, etc.

Ces deux questions sont évidemment liées : certaines catégories de réponses à la première question présélectionnent de facto certains types de réponses à la seconde.

3.1 La gestion des identités

La question est de savoir pour qui (quel agent) va-t-on créer une identité dans un progiciel métier. Cela peut paraître trivial, mais un agent travaillant à la DAF n'a pas à disposer d'une identité dans un DPI, sans même parler de quels droits il aurait. Cette question de la création d'ID est intimement liée au processus manuel ou automatisé de création.

Il existe globalement trois façons de créer les ID dans un progiciel métier :

3.1.1 ID1 : la création d'ID intuitu personae

Cela consiste à créer - la plupart du temps à la main - une identité pour Pierre, une autre pour Paul, etc. Ce mode est parfaitement valable dans le cas d'un très petit nombre d'utilisateurs. Même dans un CHU, le nombre de contrôleurs de gestion se compte souvent sur les doigts des deux mains, même dans un gros CHU le nombre d'agents à la médecine du travail excède rarement 10 à 20 accès nommés, même en comptant les personnels administratifs et soignants : le fait de créer à la main (c'est-à-dire sans le recours à un algorithme) des ID uniques pour chaque utilisateur et de leur attribuer des accès nominatifs est donc une solution tout à fait viable.
Le principal inconvénient est que le processus de suppression est aussi manuel. Une révision annuelle des comptes est donc indispensable si l'on ne veut pas que perdurent les ID de personnes ayant quitté la structure depuis des années.

Il est cependant important de préciser que cette attribution intuitu personae est faite pour éviter d'implémenter un

processus d'alimentation automatique des ID à partir de la base RH sur les critères d'appartenance service / UF / métier. Pour quelques individus, la mise en place d'un tel processus automatisé est possible mais coûteuse du fait du « ticket d'entrée technique » ; la gestion « à la main » est donc plus simple. Mais cela ne dispense pas pour autant de vérifier, au moment de créer un ID/MDP, que la personne est bien éligible : en d'autres termes, ce mode de gestion devient une anomalie lorsque la seule justification de la demande d'accès pour un agent est « parce que c'est lui ».

Indispensable revue des comptes

Il est courant de voir ce mode de gestion mis en œuvre même pour des progiciels avec un grand nombre d'utilisateurs. Par exemple, pour la gestion RH qui peut être utilisée par 100 ou 200 agents (dans un CHU, c'est courant), si le logiciel RH n'est pas automatiquement provisionné par un IAM ou si le DRH préfère une gestion manuelle des ID/MDP.

Dans ce cas, le risque est évidemment de laisser des ID/MDP perdurer lors du départ ou de la mutation d'un agent dans une autre fonction. Ce n'est pas pour rien que les Commissaires aux Comptes exigent une revue annuelle des comptes utilisateurs lorsqu'ils tombent sur ce mode de fonctionnement.

3.1.2 ID2 : la création d'ID par groupes d'utilisateurs

Dès lors que le nombre d'utilisateurs devient important (plusieurs dizaines) et/ou changent régulièrement (turn-over), le mode ID1 n'est plus gérable. On recommande souvent d'attribuer des ID à des groupes ou profils d'utilisateurs, qui peuvent être calculés à partir d'éléments connus des RH tels que le métier, le diplôme, le grade, l'appartenance à un service, etc.

Le principal avantage de ce mode est qu'il reporte sur le processus RH la question de savoir qui est légitime ou pas à être classé dans tel ou tel profil, ce qui est fondamentalement une des missions du processus RH. Le principal inconvénient est que les notions de métier, diplôme, grade peuvent rapidement aboutir à des casse-têtes d'une grande complexité : qui des « faisant fonction », qui des diplômes multiples, quid de ceux dont le métier n'a rien à voir avec le diplôme d'origine, etc. La combinatoire peut très vite devenir quasi inextricable, et dans la plupart des cas, on constate que les ambitions de départ (calculer l'appartenance à un groupe à l'aide d'une fonction complexe) se heurtent aux besoins réels et que l'on n'attribue pas des droits en faisant confiance à une équation différentielle du 8ème degré.

3.2 La gestion des habilitations

Les politiques d'accès ou d'habilitation aux données métier, quel que soit le secteur, se classent globalement en quatre catégories.

3.2.1 HAB1 : les habilitations intuitu personæ

Il s'agit d'attribuer des habilitations spécifiques pour chaque utilisateur nommé dans le logiciel. Ce mode existe de façon courante, et il ne constitue pas une anomalie de fonctionnement.

C'est le pendant de ID1 côté habilitations : lorsque le nombre d'utilisateurs d'un progiciel métier est très restreint et bouge peu, il est tout à fait envisageable d'attribuer des droits à une liste nommée de personnes. Dans l'exemple ci-dessus des contrôleurs de gestion, cela consisterait à attribuer la visibilité sur les informations RH à tel contrôleur, sur les informations financières à tel autre, sur l'activité du laboratoire à un troisième, etc. Ce mode est, la plupart du temps, bloquant : toute personne n'ayant pas un ID/MDP et les habilitations qui vont avec n'accède pas à une donnée.

Indispensable politique d'habilitations
Déployer ce genre de fonctionnement n'évite pas de devoir formaliser une politique d'habilitations, sous peine de voir l'informaticien local devenir le baron local qui décide de qui a accès à quoi - ou pire que tout le monde décide pour tout le monde.

3.2.2 HAB2 : contrôle à priori strict

Il s'agit du mode à avoir été implémenté le premier dans les premières générations de DPI au milieu des années 2000. Ce n'est rien de moins que l'industrialisation du mode précédent, industrialisation obtenue en se basant non pas sur des personnes ou agents, mais sur des profils génériques que l'on nomme aussi des rôles. Le principe est simple : les habilitations sont attribuées à des groupes d'individus et décrivent qui (ID) peut avoir accès à quoi (la donnée), toute personne n'appartenant pas à ce groupe est techniquement bloquée dans l'accès à la donnée.

Principes
Sans rentrer dans le sujet des modèles théoriques des rôles (RBAC, Or-BAC, etc.), l'idée est de procéder en au moins deux étapes :

• **étape 1** : tout utilisateur du progiciel se voit rattaché à un rôle, en fonction des informations telles l'appartenance à un service ou pôle, le niveau hiérarchique, le métier, le diplôme, etc. ; par exemple on peut imaginer les rôles « Chirurgien », « Infirmier anesthésiste », « Infirmier », « Aide-soignant », « Secrétaire médicale », etc. ;

• **étape 2** : à un rôle correspond une matrice de droits ou d'habilitations, qui donne ou pas accès à telle ou telle information ; par exemple le rôle « Chirurgien » donne accès à la feuille de bloc opératoire et au module de prescription médicamenteuse, mais pas au volet administratif du patient ; à contrario, le rôle « Secrétaire médicale » donne accès au module administratif du DPI mais pas aux modules de prescriptions ; (ce ne sont que des exemples bien entendu) ;

Une fois que chaque agent (et les informations RH nécessaires au « calcul » de son rôle) a été collecté, le reste (à savoir l'affectation de

tous les agents à la matrice des rôles et le calcul automatique des droits d'en connaître) peut facilement être automatisé.

On nomme ce type de contrôle « à priori » car si le système dit que telle personne n'a pas accès à telle donnée, elle n'y a physiquement pas accès dans le progiciel, ce ne sont pas simplement des messages d'alerte. Si nous reprenons la métaphore automobile, le véhicule serait physiquement bridé à 130 km/h sur autoroute et 50 km/h en ville.

Contrôle à priori et confidentialité

En général, ce mode de contrôle constitue un excellent choix lorsque les données traitées ont pour critère de sécurité principal la confidentialité, au détriment des deux autres aspects (I et D) comme une donnée d'infection VIH par exemple, ou une donnée concernant l'état psychiatrique de la personne. Le problème survient lorsqu'un DPI comporte à la fois des données de ce type, mais aussi des données pouvant servir à une prise en charge médicale en urgence, pour lesquelles I et D reviennent au-dessus de la pile.

Les inconvénients du modèle

Ils sont nombreux, à commencer par la difficulté de l'étape 1 susnommée : s'il peut être relativement facile, dans une DRH, de déterminer des rôles en fonction des affectations des agents (paye, gestion des carrières, maladie, etc.), les équipes de soins sont souvent beaucoup plus difficiles à faire rentrer dans un moule uniforme.

Entre les praticiens qui ont plusieurs spécialités, les cadres de santé qui sont « faisant fonction » (sans le diplôme mais en assumant tout de même le poste), les professions totalement transversales (urgentistes, radiologues, kinésithérapeutes, infirmières hygiénistes, etc.), l'expérience montre que la loi de Paréto fonctionne dans le mauvais sens : 80 % des personnels sont facile à faire rentrer dans une classification des rôles, mais on dépense une énergie considérable avec les 20 % restants.

L'étape 2 n'est pas simple non plus : sans même parler des exceptions, la rédaction du corpus initiale de règles (définition de quel rôle donne accès à quoi) est d'une rare complexité. Toutes les tentatives que j'ai vues dans les établissements que j'ai côtoyés se sont soldées par un échec : au départ tout le monde pense que cela tient en quelques lignes, mais dans les faits on aligne rapidement des pages et des pages et on continue de débusquer des cas particuliers à chaque échange, à tel point que le corpus des exceptions finit par être 10 fois plus gros que le corpus des règles.

L'autre inconvénient, c'est que dès que l'accès à une donnée est physiquement bridé, les utilisateurs contournent d'une manière ou d'une autre, sans préjuger de la pertinence de ce contournement : prêts de mots de passe, sessions utilisateurs laissées ouvertes, etc.

Ce mode n'est gérable que dans les petits établissements, ou les établissements avec une faible diversité des activités tels des établissements SSR, des EHPAD. Dans un CH généraliste (sans même parler d'un CHU), ce mode est voué à l'échec.

Les cas d'usage pertinents

Il existe cependant des cas d'usage qui se prêtent parfaitement à ce modèle : jeu de données parfaitement identifié et à forte contrainte de confidentialité, acceptation d'une perte importante de disponibilité, petit nombre d'utilisateurs, contraintes réglementaires fortes, etc.

3.2.3 HAB3 : contrôle à priori avec bris de glace

Il s'agit d'une déclinaison ou amélioration du mode précédent. Le mode de fonctionnement est identique à un détail près : si l'accès à la donnée est techniquement bloqué, il existe un dispositif de type « bris de glace » qui, lorsqu'il est déclenché par l'utilisateur, lui donne accès à ce qu'il ne peut pas consulter ou modifier dans le fonctionnement normal.

Ce serait, par exemple, l'accès aux données d'un patient en principe masquées mais qui nécessitent d'être consultées pour la prise en charge médicale.

Concrètement, le déclenchement du bris de glace génère un ou plusieurs messages d'alertes et des traces techniques, qui sont stockées et - en principe - analysées et exploitées à postériori.

Les inconvénients du modèle

Si, sur le papier, ce mode semble satisfaisant, dans les faits, il a pour principal inconvénient de générer énormément de bris de glace : sans analyse systématique de ces bris de glace, le système est détourné de son esprit initial.

Les bris de glace, l'inflation constante

Pour élément d'analyse, le nombre de bris de glace journaliers dans un CHU - et à fortiori dans un GHT qui aurait mis en place un DPI commun - varie entre 1000 et 10 000. Dit autrement, il arrive plusieurs milliers de fois par jours qu'un professionnel de santé (corps médical ou corps soignant) ait besoin d'accéder à une donnée médicale d'un séjour qui ne se trouve pas dans son périmètre initial de prise en charge. Besoin de vérifier une prescription faite dans un autre service, besoin de vérifier des antécédents médicaux, ce nombre illustre bien la limite du système de bris de glace qui surviennent à une telle fréquence que l'analyse en devient particulièrement complexe.

3.2.4 HAB4 : contrôle à posteriori

Devant les difficultés inhérentes au mode de contrôle à priori, certains établissements de santé ont commencé à mettre en place un mode de contrôle à posteriori, qui est aux habilitations ce que les radars de vitesse sont à l'automobile : les véhicules ne sont pas physiquement bridés à 130 km/h, potentiellement une voiture peut monter au-delà mais c'est interdit pas les textes (la loi) et il y a des contrôles.

Dans les faits, cela signifie que l'ensemble du personnel médical et soignant dispose d'un ID/MDP d'accès au DPI avec des droits extrêmement étendus (chaque personnel du corps médical a par exemple un accès à tous les dossiers de tous les patients), mais les textes (règlement intérieur, Code de la Santé Publique, Charte Informatique, etc.) précisent que seul l'accès aux données des patients pris en charge par la personne est autorisé et il y a des contrôles.

Ces contrôles vont être réalisés à partir des traces générées par le DPI à chaque action utilisateur : ouverture d'une session, accès à un dossier patient, consultation ou modification d'une donnée, etc. La possibilité juridique d'effectuer des contrôles sur traces doit être stipulée dans

la Charte Informatique, sinon ces contrôles n'auraient aucune valeur, voire seraient même carrément illégaux.

Cartographie des rôles

Ce mode de contrôle ne dispense pas d'avoir une cartographie précise des rôles, toujours basée sur des critères telle l'appartenance à un service ou pôle, le métier, le diplôme, etc. En effet, pour qu'il y ait contrôles - les plus automatisés possibles sinon cela va devenir très chronophage, surtout dans un CHU - il faut les baser sur des éléments « calculables ». La seule connaissance du personnel médical par un DIM ou un contrôleur ne suffira pas. La trace, qui comprend l'identité de l'utilisateur qui en est à l'origine, va devoir être couplée à la base des rôles pour pouvoir déterminer si l'accès à la donnée patient est légitime ou pas.

Aménagements possibles

Il est courant que la politique d'accès implémentée ne soit pas « tout accessible pour tout le monde », mais que les corps soignant et administratifs aient des restrictions. Par exemple que seules les données des patients du service soient accessibles en mode « contrôle à postériori » mais que les données des autres patients des autres services soient physiquement bridées. C'est un choix, et cela ne résout bien entendu pas la question des professions transversales : infirmières de pool, etc.

Ce mode s'accompagne généralement d'une notion de patient ou séjour en hyperconfidentialité : si tout le monde peut techniquement tout voir, les patients ou séjour en question nécessitent, pour être consultés, le déclenchement d'un bris de glace équivalent à HAB3. La seule différence est en fait le positionnement du blocage : en sortie de l'unité d'affectation pour HAB3, à l'arrivée sur le DPI d'un patient ou séjour hyperconfidentiel dans HAB4.

Les inconvénients du modèle

La confiance n'exclut pas le contrôle, et les sanctions constituent un élément majeur de ces contrôles et de la confiance qui en découle. Dans certains domaines ou certains établissements, un agent pris la main dans le sac à consulter des données qui ne le regardent pas se voit infliger une sanction qui peut aller jusqu'au licenciement pour faute.
Dans le monde de la santé, les licenciements, même pour cas avérés, sont rarissimes et dégradent la confiance à la fois des utilisateurs de ces DPI, et des usagers.

L'autre point majeur est que les contrôles nécessitent des ressources humaines importantes. On ne mène pas des contrôles régulier et systématiques, en plus des contrôles sur suspicions d'indiscrétion, dans un CHU avec 1/2 ETP de technicien d'information médicale. Sans ressources pour les contrôles, on retombe dans le même travers du manque de confiance dans l'outil. À noter que ce besoin de ressources pour les contrôles est exactement le même dans HAB3, dans les faits les établissements qui sont dans le mode HAB3 ont tendance à moins effectuer ces contrôles, s'abritant derrière une trop grande confiance dans le mode bris de glace.

L'inconvénient majeur du mode de contrôle à postériori - accentué par l'absence de contrôles et de sanction - est que quand le mal est fait, il est trop tard. Quand un patient constate que son statut VIH positif a fuité par indiscrétion, quand un agent d'un hôpital qui se fait suivre dans le service psychiatrie de ce même hôpital constate que tous ses collègues sont au courant, il est trop tard.

3.3 Evolution des usages

A titre indicatif, voici une matrice des croisement ID/HAB.

Gestion des ID	Gestion HAB	Possible
ID1	HAB1	Oui
	HAB2	Oui
	HAB3	Oui
	HAB4	Oui
ID2	HAB1	Non
	HAB2	Oui
	HAB3	Oui
	HAB4	Oui
ID3	HAB1	Non
	HAB2	Oui
	HAB3	Oui
	HAB4	Oui

La tendance générale est d'aller de ID1 vers ID2 ou ID3, ce qui s'explique aisément par le fait que de plus en plus d'agents ont besoin de l'outil informatique pour travailler. Il y a bien entendu des exceptions, qui s'expliquent par le caractère restreint d'un progiciel, la nature particulière des données traitées, etc : qu'un logiciel de médecine du travail soit en mode ID1 est normal, qu'un DPI de CHU soit en mode ID1 est une anomalie.

Pour le volet habilitations, exceptées les mêmes cas d'usages qui relèvent de HAB1, le mode HAB2 pour les DPI est en voie de disparition et la quasi-totalité des CHU et gros CH se situent entre HAB3 et HAB4 (avec quelques nuances dans les déclinaisons).
La grande question en ce début de décennie est de savoir si les coopérations médicales massives entre établissements (GHT, collaboration entre des prises en charge de spécialité et le CH/CHU généraliste régional, etc.) pourront s'accommoder du mode HAB3 ou devront forcément passer au mode HAB4 - étant entendu que, côté ID le mode ID1 est totalement impossible et que l'on ne peut être que sur du ID2. Cette question est absolument centrale et conditionnera pour partie les évolutions des réseaux de soins, ce qui est le sens de l'histoire de la médecine.

4. Les processus socle

Quel que soit le modèle choisi - ou toute combinaisons de ces modèles -, il y a un certain nombre de processus à mettre en place, qui constituent le socle des habilitations d'accès, et ce quel que soit le domaine fonctionnel : RH, finances, DPI, etc. Ce socle est une déclinaison du PDCA (Plan Do Check Act) cher aux qualiticiens, et c'est également la vision qu'utilisent les Commissaires aux Comptes pour les habilitations qui concernent les données qu'ils contrôlent (essentiellement celles correspondant à des flux financiers).

4.1 Le dispositif

4.1.1 Phase Plan

Cela consiste à décrire la politique choisie dans un document clair. Cela peut tenir en 10 lignes (« seuls les médecins affectés au service de médecine du travail auront accès aux données du progiciel »), cela peut être plus complexe. La question de savoir si ce seront les modes ID1, etc., HAB1, etc. qui vont être retenus, fait partie de ce document.

Dans l'idéal, il faut décrire des profils métier : « les agents en charge de la paye », « les agents en charge de la gestion des avancements », « les médecins du bloc opératoire », etc. Il faut évidemment proscrire toute référence à des personnes. Il va également être nécessaire de mettre en place un dispositif de contrôle des traces : outils, moyens, plan de contrôle, organisation, responsable, etc.

4.1.2 Phase Do

Cela consiste à dérouler les modes ID et HAB retenus dans la politique susnommée. Cette phase d'automatisation peut rapidement devenir longue et complexe : dans le cas d'un fort taux de turn-over de personnels (dans les CHU, il est aux environ de 10 % si on inclut les personnels de remplacement), il va être indispensable de coupler ceci à un IAM (voir plus bas).

4.1.3 Phase Check

Il va être nécessaire de procéder à des revues annuelles de :

• la politique à proprement parler ; le document décrit en phase Plan doit faire l'objet d'une réévaluation périodique, idéalement tous les ans ;

• l'affectation des personnes aux profils métier.

Il conviendra ensuite de dérouler le plan de contrôle des traces.

4.1.4 Phase Act

Toute anomalie identifiée en phase Check doit bien entendu être corrigée : agent ayant quitté ses fonctions et dont les ID/MDP sont toujours actifs, profil métier trop large, etc.

Charge de travail

Le dispositif décrit n'est pas forcément lourd à mettre en œuvre ou à faire vivre. Dans un établissement de taille moyenne comportant peu de profils différents (médicaux ou soignants) et donc peu de spécialités différentes, la politique d'accès au DPI peut tenir en 3 pages, la révision de la politique peut tenir en une heure à peine et la revue des comptes utilisateurs (même s'il y en a une centaine) peut ne nécessiter que 2h maximum.

Et si on est dans le cas d'un gros CHU comportant des centaines de profils et des milliers d'utilisateurs, la revue des comptes peut être réalisée par échantillonnage : tous les trimestres, par exemple, on vérifie les comptes de tel ou tel pôle.

4.2 Les pièges

Quel que soit le modèle d'habilitations retenu, les pièges sont globalement les mêmes.

4.2.1 L'immobilisme

Sans revue périodique, tout système finit par contenir des comptes d'agents ayant été mutés, ayant quitté leur fonction, partis à la retraite, etc. Les revues périodiques des comptes utilisateurs ont pour seul objectif de « faire passer la voiture balais » pour ne pas laisser traîner ces comptes, qui constituent une porte d'entrée rêvée pour les attaquants.

4.2.2 La tâche d'huile

Un des travers les plus courants est l'extension progressive et rampante des droits utilisateurs. Cas concret : un service signale l'arrivée de tel cadre de santé XXX à qui il faut affecter non pas les droits de tel profil métier (ce qui serait logique et sain), mais « les mêmes droits que Mme YYY ». Et puis le service rappelle deux jours plus tard en demandant de rajouter en plus les droits d'accès à telle donnée, telle donnée, telle donnée. Et un mois plus tard arrive M ZZZ pour lequel on demande les mêmes droits que Mme XXX, et de proche en proche tout le monde finit par avoir tous les droits sur tout.

La seule contre-mesure à ce type de dérive est de se baser sur des profils et non les droits de tel ou tel agent.

4.2.3 La balkanisation des profils

Un contournement courant lorsque la politique des profils est stricte est de finir par créer autant de profils que d'utilisateurs : j'ai vu un logiciel de gestion des rendez-vous qui comportait 1000 utilisateurs et 1000 profils : inutile de dire que l'étape Plan (définition de la politique) était depuis longtemps passée à la trappe. La seule contre-mesure est de s'appuyer sur une politique stricte et de ne pas s'en écarter.

4.2.4 Confusions dans le processus de décision

Une question centrale et récurrente est : qui décide d'une politique d'habilitation sur une typologie de données métier ?

Certainement pas la DSI, qui n'est pas là pour décider du contenu (les données et qui y accèdent) mais pour mettre en place des outils (le contenant).

Certainement pas tous les agents du service ou pôle métier en question : si on constate que tous les agents d'une DRH sont en position de demander une modification ou extension des droits de n'importe quel autre agent - y compris eux-mêmes -, cela relève d'une grosse anomalie (que les Commissaires aux Comptes ne manqueront pas de signaler sur leur périmètre de contrôle).

Les bonnes pratiques recommandent de désigner comme responsable de cette fonction de définition une seule personne ou un groupe de travail : si un décideur n'a pas physiquement le temps de s'atteler à cette tâche, rien ne lui empêche de déléguer à un cadre. Dans tous les cas, la définition d'une politique d'habilitation relève de la MOA et certainement pas de la MOE.

Séparation des rôles

Pour éviter les discussions où le ton monte entre un agent qui estime (à tort ou à raison) avoir besoin de tel ou tel accès, et le service qui gère physiquement ces accès (la cellule habilitation, la hot line, ou une équipe dédiée, souvent rattachée à la DSI d'ailleurs), une bonne pratique est de

séparer strictement celui qui décide d'une politique d'habilitation (le métier) et celui qui l'exécute (cette équipe susnommée). Ainsi devant toute demande qui sortirait des clous, la cellule habilitation pourra se dégager de la pression en affirmant qu'elle n'a pas le pouvoir de déroger à une politique décidée par la MOA.

Dans les meilleures pratiques que j'ai pu voir, la MOA des habilitations est confiée à un groupe de travail pluridisciplinaire : représentant métier, RSSI, DPO, décideur, etc. N'est-ce pas le signe d'un processus démocratique mature que d'échanger, de débattre et de parvenir à un consensus ?

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

5. Le DPI

5.1 Généralités

Le DPI constitue le support informatique du cœur de métier d'un établissement de santé, public ou privé. Il est supposé rassembler, pour chaque patient, l'intégralité des données médicales connues du patient en question, ce qui comprend aussi bien des données administratives (patronyme, date de naissance, adresse, etc.) que des données de santé généralistes (poids, taille, etc.), des « fiches générales » telles les allergies ou les antécédents médicaux, mais aussi des données classées par spécialités telles la cardiologie, l'urologie, etc.

Le DPI comporte donc des sections administratives, santé généraliste, spécialités médicales et sert aussi bien au support de facturation qu'à la prise en charge en médecine « classique », aux urgences médicales, à la psychiatrie, etc.

5.2 Les éléments de la prise de décision

5.2.1 La notion de perte de chances

Il est primordial d'intégrer à ce stade la notion de perte de chances. Chaque fois qu'une donnée est rendue inaccessible à un praticien qui prend en charge le patient, ce dernier subit une « perte de chances » au sens où le praticien va devoir prendre des décisions en l'absence d'informations qui pourraient être cruciales, changer totalement son diagnostic ou les actes qui en résultent. Lorsqu'un patient souhaite que son dossier médical bénéficie d'un statut « confidentiel ++ » (ce que permettent la plupart des DPI), on lui fait en général signer un document qui précise la perte de chances qui en résulte et le fait qu'il en assume les conséquences.

Prescrire un traitement médicamenteux pour un patient qui arrive en consultation d'ophtalmologie sans que le statut VIH positif du patient ne soit connu du praticien, peut avoir des conséquences irréversibles, tout comme prendre en charge aux urgences médicales un patient sous traitement médicamenteux inconnu de l'urgentiste.

5.2.2 Arbitrage nécessaire

Sur le plan de l'arbitrage DIC évoqué dans le paragraphe sur les fondamentaux, le DPI est donc un cauchemar absolu, aussi bien du RSSI, du DPO que bien entendu du DIM ou du Président de CME. Et ce surtout quand il s'agit du DPI d'un gros établissement qui héberge à la fois de la chirurgie, de la psychiatrie, de la médecine interne, du médico-social, de la recherche médicale, etc. Chacun de ces secteurs a des contraintes qui lui sont propres et qui sont fondamentalement en opposition avec d'autres contraintes, tout aussi légitimes : la psychiatrie met la confidentialité au-

dessus des autres critères, pour les urgences médicales c'est exactement l'inverse, avec la disponibilité comme priorité.

5.2.3 La question du choix

Il est enfin important de réaliser que la décision de confidentialité des données médicales d'un patient donné, lorsqu'elle entraîne comme nous venons de le voir une perte de chances, ne peut relever que du patient lui-même. En aucun cas la décision ne peut être prise par l'établissement, et encore moins par le biais d'un processus automatisé (par exemple « tous les patients prisonniers sont de facto en hyper confidentialité »). Ceci sans préjuger des dispositions et obligations déjà prévues par la loi bien entendu.

5.3 Historique de la question des habilitations

Lorsque les premières générations de DPI ont été déployées, la question des habilitations s'est forcément posée et n'avait été anticipée quasiment nulle part : on partait la plupart du temps d'établissements qui avaient été informatisés en mode « silo » (chaque service possède son mini-DPI) et ce sujet n'avait jamais été à l'ordre du jour.

Lorsqu'il a fallu mettre toutes les données dans le même DPI, il y a eu à beaucoup d'endroits des oppositions farouches du corps médical : tel praticien ne voulait pas partager « ses » données de « ses » patients avec le praticien du service d'en face.

Quand l'histoire fait rire

Lorsque l'on raconte cet épisode à de jeunes chefs de clinique récemment sortis de la Faculté, ils sont proprement ébahis devant la réaction de leurs aînés. Mais cette réaction était compréhensible à l'époque, il s'agit avant tout d'un problème de maturité organisationnelle et pas d'informatique, et la maturité ne se décrète pas : elle arrive avec le temps, « il faut que jeunesse se passe ».

Dans les faits, les premiers DPI ont été implémentés sur le modèle du contrôle à priori strict (HAB2), ce qui était un choix logique à l'époque. Très rapidement, surtout dans les gros établissements, ce mode est devenu intenable et à l'heure où ces lignes sont écrites aucun CHU - sauf erreur - et aucun gros CH de France n'a conservé le mode HAB2 : tous sont passés dans le mode HAB3 ou HAB4.

5.4 Vers un à posteriori, avec des exceptions

Partout et en tous cas dans tous les établissements généralistes, le constat est fait de la limite du modèle de contrôle à priori strict (professions transversales, exceptions régulières, etc.), et du nécessaire passage au mode de contrôle à priori avec bris de glace ou à posteriori (HAB3 ou HAB4).

La notion d'équipe médicale élargie
Le Code de la Santé Publique reconnaît la notion d'équipe médicale élargie. Cela signifie qu'un patient n'est pas pris en charge, dans un établissement de santé, par un médecin et / ou un personnel soignant, mais par une équipe qui peut être large (UF, service, pôle), d'autant plus que l'établissement est pluridisciplinaire et que le patient est polypathologies. Dans ce contexte, le mode HAB2 est tout simplement impossible.

Si cet opus avait été écrit en 2015 et pas en 2020, la conclusion aurait été de passer massivement vers HAB4. Cela étant, la réalité est un peu plus nuancée et la réflexion pas finalisée à ce jour, les pistes de solutions évoquées sont susceptibles d'évoluer dans les prochaines années, même si dans les grandes lignes on sait à peu près où l'on va.

Globalement, nous en sommes à ce stade de la réflexion :

• nécessité d'un passage massif vers le contrôle HAB3 ou HAB4 pour toutes les données médicales hors exceptions ;

• les exceptions connues à ce jour sont : la psychiatrie, certains éléments de la prise en charge médico-sociale et tout ce qui relève de l'hospitalisation sous X ; pour ces domaines, il faut envisager de les isoler du mode général « à posteriori » pour en faire des sanctuaires « à priori » (HAB3) voire dans certains cas (rares) sur le mode « intuitu personae » ;

• pour ces exceptions, une partie des données (en particulier les éléments de prescription médicamenteuse) doivent tout de même rester en mode HAB3 ou HAB4 ; l'exception ci-dessus comporte donc elle-même une exception, ce qui rend le paramétrage des DPI particulièrement délicat ;

• tout DPI doit pouvoir implémenter un mode « hyper confidentialité », au choix du patient et de lui seul, et qui bascule tout ou partie du DPI du patient (dossier généraliste, séjour, ou tout le DP) dans un mode « à priori » (accès réservé aux praticiens d'un service), voire à une liste nommée (mode intuitu personae) ; ce mode doit permettre de masquer le contenu d'un DP entier ou d'un séjour, mais aussi de masquer l'existence même de ce dossier ou séjour à ceux qui n'ont pas le niveau d'habilitations requis. La perte de chance qui en résulte doit avoir été portée à la connaissance du patient, avec traçabilité, signature, etc. ;

• tout DPI doit implémenter un mode de gestion « patient sensible » ou « séjour sensible » : il s'agit de patients ou séjours qui ne sont pas en mode hyper-confidentialité (qui induit une perte de

chance), mais qui doivent faire l'objet d'un soin particulier à la confidentialité de leurs données médicales : les agents hospitalisés dans leur propre établissement, les VIP, les prisonniers, etc. ;

• fonction « bris de glace » indispensable, sur tous les éléments du DPI, y compris les exceptions susnommées. Le déclenchement de ce mode par le praticien doit générer les alertes qui permettent de ne pas l'activer par erreur, et ce déclenchement doit être auditable ;

• outil de traçabilité intégré au DPI et disposant de fonctions avancées (voir plus bas) ;

• la capacité d'analyse des traces est un élément majeur, qui permettra de trancher entre le mode HAB3 ou HAB4. En effet, le mode HAB3, s'il semble plus satisfaisant sur le papier, a pour principal inconvénient de générer beaucoup d'accès en mode bris de glace, qui vont constituer un détournement rapide du système sans politique stricte d'analyse des traces (et de sanction le cas échéant) ;

5.5 Les questions en suspens

Le principal problème, non résolu à ce jour, est lié à la confrontation au sein d'un même DPI, de professions ou spécialités médicales qui ont des besoins totalement antagonistes en matière de sécurité des données.

5.5.1 Statut particulier de la donnée médicale psychiatrique

Il serait hasardeux de nier le caractère extrêmement sensible d'un diagnostic de psychiatrie. Alors que dans une prise en charge « classique », les données collectées concernent le patient et lui seul (cardiologie, urologie, etc.), la particularité de cette spécialité est que le patient ne parle pas forcément que de lui, mais aussi potentiellement de son entourage (père violent, oncle violeur, etc.).

Et en termes de confidentialité et surtout d'impact en cas de rupture de cette confidentialité, on est au même niveau que celle d'un statut VIH du patient, qui bénéficie quant à elle du statut « sous X » de la prise en charge médicale.

On touche d'ailleurs à la limite de la définition de ce qu'est, ou pas, une donnée médicale. Si ma correction visuelle ou mon niveau de cholestérol sont indiscutablement des données médicales (cela apporte une information sur mon état physique), le fait que je sois passé dans le service de cardiologie en consultation n'en est pas une (on ne peut rien en déduire). En revanche, l'information du passage dans certains services (secteur IVG, psychiatrie, etc.) est une information médicale - autrement dit certaines « méta-informations » deviennent vite des données de santé.

5.5.2 DPI généraliste versus DPI de psychiatrie

Lorsqu'un établissement de santé est un établissement psychiatrique sans autre spécialité médicale, le mode d'habilitations le plus couramment observé est le mode à priori. Cela se complique lorsqu'un même DPI abrite des données médicales utilisées à la fois par des urgentistes (I et D prépondérants) et des psychiatres (C prépondérant).

Certes, il est possible, si le progiciel le permet, de choisir le mode à posteriori pour toutes les données médicales « standard » et d'isoler la partie psychiatrie dans un mode à priori ou intuitu personae. Mais cela ne résout pas tout : il y a forcément des données, produites par les psychiatres, et qui sont éminemment transversales dans une prise en charge. L'urgentiste n'a pas forcément besoin de savoir que le patient est schizophrène (et encore, tous les urgentistes ne sont pas d'accord sur ce point), mais il a, en revanche, besoin de savoir si ledit patient était sous traitement médicamenteux. Et bien évidemment les psychiatres rétorquent que la connaissance du traitement en question pourra permettre de déduire la schizophrénie du patient. Bref on ne s'en sort pas.

5.5.3 Positions antagonistes

D'une part, la position des psychiatres - rendre totalement confidentiel le passage en psychiatrie, également pour la partie médicamenteuse de ce séjour - revient à adopter un mode d'hyper confidentialité pour un séjour, donc à induire une perte de chance médicale, décision qui ne peut relever que du patient (ou de ses représentants légaux le cas échéant). Une bonne partie des professionnels de santé (non psychiatres) avec qui j'ai pu échanger pense que le volet psychiatrie du DPI n'a pas à être plus confidentiel que les autres volets, au motif qu'une prise en charge médicale est forcément globale et que l'on ne peut pas découper le corps humain par bouts.

D'autre part, on constate que les agents d'établissements généralistes (souvent des CHU) qui ont besoin de consultations en psychiatrie, vont souvent se faire suivre dans un autre établissement que le leur, ce qui en dit long à la fois sur le caractère sensible de cette spécialité - le simple fait de savoir que l'on est suivi en psychiatrie fait que certaines personnes vous regardent de travers - et la capacité quasi nulle des gros établissement à garantir la confidentialité des données médicales de leurs propres agents, sans parler de celle de la famille de ces mêmes agents, de leurs voisins de palier, etc. Les réserves des psychiatres sont donc tout à fait fondées.

5.5.4 Les pistes

La réponse à ce dilemme ne peut venir que du corps médical : il n'appartient pas au RSSI, au DPO ou à la DSI d'y répondre. Ce débat relève du corps médical dans son ensemble et de la Direction Générale, et doit absolument être collégial.

Il semble que le passage au mode HAB3 ou HAB4 aille dans le sens de l'histoire, et avec des exceptions parfaitement identifiées susnommées. Mais ce qui est certain, c'est que le passage au mode à posteriori pour ces données est conditionné par :

- la capacité des DPI à cloisonner certaines spécialités et à identifier des patients ou séjours comme « sensibles » (hors statut d'hyper confidentialité), ce qui suppose un niveau fonctionnel ;

- la capacité des équipes opérationnelles en charge du contrôle des traces à exploiter les données, ce qui suppose des moyens humains ;

- la capacité des établissements à sanctionner les contrevenants, ceci pouvant aller jusqu'au licenciement, ce qui suppose une volonté politique.

5.6 Le cas des GHT

Le passage en GHT rend la question encore plus brûlante. Si antérieurement un établissement psychiatrique gérait seul ses habilitations, le passage à un DPI de GHT va, de facto, poser la même question du mode d'habilitations que pour les gros CHU multi-activités.

Certes le passage au DPI de GHT est flou et on observe plusieurs tendances : certains GHT font table rase des DPI locaux pour en imposer un seul (un nouveau ou un existant supposé « tenir la charge »), d'autres GHT préfèrent conserver les DPI locaux, et monter un mini DMP de GHT alimenté par tout ou partie des données issues des DPI locaux, d'autres GHT enfin prennent la voie du milieu en réalisant des acquisitions de DPI sectoriels pour couvrir toute la psychiatrie, toute la médecine générale, etc.
Mais dans les trois cas, l'esprit de la loi de santé 2016 qui a mené à la construction des GHT est sans aucune ambiguïté : il faut créer des filières médicales et prendre les patients de façon coordonnée, ce qui implique de toute manière de partager des données médicales entre spécialités hétérogènes.

La question des habilitations dans un environnement multi-spécialités est donc remise à l'ordre de jour avec les GHT. Certains pensent d'ailleurs, grâce au recul des premiers DPI d'il y a 15 ou 20 ans, que la question du DPI de GHT (quelle que soit l'option retenue) se fera, ou ne se fera pas, selon la capacité des institutions à régler cette question des habilitations.

5.7 Limite du modèle DMP

Récemment, un confrère me faisait la remarque suivante : pourquoi n'est-il pas possible de mettre en œuvre une gestion des traces au sein d'un DPI, identique à ce qui se pratique pour le DMP ?

La question est tout à fait pertinente : pour les citoyens qui ont ouvert un DMP, il est possible de visualiser qui a eu accès à quoi, au sein des personnes qui disposent d'un accès DMP (potentiellement toute personne détentrice d'une carte CPS à quelques nuances près). Pour un DPI interne d'établissement de santé, cela me semble difficile à mettre en place et ce, pour plusieurs raisons.

La première, et qui n'est pas si facile que cela à gérer, est qu'il va falloir ouvrir en mode Web le DPI en question pour que les patients puissent le consulter à distance (ce n'est pas la partie la plus compliquée, si tant est que l'éditeur propose un module Web, ce qui est loin d'être le cas de tous), mais surtout il va falloir gérer les accès des patients : création de ID/MDP temporaires, distribution de ces ID/MDP, gestion des procédures de vérification (envoi d'un code SMS en guise de MFA, ce qui suppose que les numéros de téléphones portables soient à jour dans la base patient), et surtout gestion des pertes /vols d'ID/MDP.

C'est cette dernière partie qui est la plus drôle : quand on demande quel service en interne va devoir gérer cela, c'est-à-dire mettre à disposition un front office patient, tout le monde pense à la DSI. Mais ce n'est pas son rôle : à part la Direction des Usagers, il n'y a pas grand monde dont la fonction « officielle » s'adapte à cette demande.

La deuxième est la quantité effroyable de personnes qui sont susceptibles - et légitimes - à consulter un dossier patient. Il y a bien entendu le corps médical et le corps soignant, mais aussi le DIM, la Qualité (pour produire des indicateurs), la Direction Juridique (dans le cadre de la gestion de contentieux), la Recherche (et tous les accès ne sont pas anonymisés), les organismes externes de contrôle (CPAM, etc.), les secrétariats médicaux, les personnels de facturation, les admissionnistes, dans certains cas la DSI (pour reproduire un dysfonctionnement signalé), les internes (pour préparer leur thèse), et cela n'en finit plus. Le risque est donc d'observer, pour certains DP, une liste à la Prévert et de tomber sur des patients qui demandent - légitimement - des explications, ce qui va être très chronophage. Certes on peut filtrer et ne montrer que la partie médicale / soignante / secrétariat des accès, mais alors quid du reste ?

Bref le sujet n'est pas si trivial, et en tout cas cette mesure ne peut se suffire à elle-même : il faudra la coupler à des contrôles internes, sur les modes précédemment décrits.

QUELQUES ASPECTS SPÉCIFIQUES À LA PSYCHIATRIE CONCERNANT LES HABILITATIONS D'ACCÈS AUX DONNÉES MÉDICALES

Par le Docteur Pierre LAFAY, Ancien Président de la CME de l'Hôpital Georges DAUMEZON

Ces dernières années, la création des GHT, et notamment la mise en œuvre du dossier patient informatique à l'échelle d'un GHT, donc accessible à un grand nombre de soignants utilisateurs, a été l'occasion de discussions autour de l'accès plus ou moins élargi au DPI. Il est apparu que les professionnels de la psychiatrie avaient souvent une vision plus restrictive de l'accès aux données que la majorité des professionnels du MCO (médecine, chirurgie, obstétrique), au point d'être moteurs dans les exigences de confidentialité de ce nouveau dispositif. Ce constat était-il seulement le symptôme d'un retard d'évolution de la branche psychiatrique du système de santé, comme l'ont caricaturé certains, ou était-il le reflet de problématiques spécifiques liées à cette discipline ? Partant de cette deuxième hypothèse, nous allons essayer de l'éclairer.

1. Stigmatisation des patients « psy » et accès aux dossiers des soignants suivis en psychiatrie

Même si cela peut paraître surprenant à l'heure où les pathologies psychiatriques sont largement documentées, diffusées et apparemment acceptées et reconnues, le fait d'être suivi pour une pathologie psychiatrique ou addictive est encore très mal vécu par nombre de patients. Nos collègues libéraux veillent souvent d'ailleurs à éviter que les patients ne se croisent en salle d'attente, précautions étrangères à la quasi-totalité des spécialités médicales. Le jugement négatif envers les personnes suivies est encore plus péjoratif si la personne a été hospitalisée à temps plein, particulièrement en psychiatrie publique. Certains patients estiment d'ailleurs qu'ils pourraient être licenciés si leur employeur apprenait ce suivi.

Aussi est-il habituel de faire hospitaliser en psychiatrie un soignant de psy ou son entourage dans un autre établissement que celui où il travaille, notamment pour respecter cette confidentialité. Mais qu'en est-il si le dossier est commun à tous les établissements et accessible à ses collègues de travail ? Au CHU de Nantes, il y a plus de 15 ans, un système automatique de confidentialité renforcée protégeait tous les patients suivis en psychiatrie (comme les détenus soignés, les patients HIV positifs et les femmes suivies au planning familial, qui pouvaient chacun être victimes de stigmatisations spécifiques).

Le non-respect de cette confidentialité est un motif récurrent de refus des soins, se rajoutant à l'ambivalence ou au déni liés aux pathologies psychiatriques ou addictives.

Ceci nous oblige à prévoir pour les professionnels des établissements du GHT (voire, à terme, des divers GHT interconnectés) une procédure d'accès au dossier psychiatrique avec contrôle a priori, restreint aux professionnels du service de prise en charge et non pas à une catégorie professionnelle.

De même, il paraît nécessaire qu'un système « bris de glace » permette à certains professionnels d'avoir accès à ce dossier malgré cette restriction (par exemple, aux urgences, face à un patient manifestant des troubles du comportement, il parait indispensable d'avoir accès à ses antécédents, psychiatriques ou autres, traitements et suivis même s'il s'agit d'un collègue de travail, car cela paraît nécessaire pour une prise en charge adaptée). Le non-accès pourrait entraîner une perte de chance importante pour le patient concerné. Hors urgences, un accès seul aux antécédents somatiques, traitements prescrits et bilans paracliniques paraît suffisant. Dans tous les cas, il apparaît utile qu'un message d'alerte informe le professionnel qu'il va consulter un dossier sensible. L'usage de la fonction « bris de glace » doit cependant entraîner un message d'alerte à l'attention du professionnel qui consulte, avec confirmation par le professionnel (contrôle a priori) mais également l'alerte du DIM avec traçage de l'accès au dossier qui permettra un contrôle a posteriori de la légitimité de cet accès. Ceci implique suffisamment de temps DIM dédié à cette mission pour l'exercer réellement

2. Besoin de notes accessibles uniquement à un professionnel

Souvent, nos patients ont besoin de vérifier le contenu du dossier, ce que nous notons des entretiens et ce qui reste dans la mémoire du soignant. Il arrive qu'ils nous demandent spécifiquement de ne pas noter certains secrets douloureux, familiaux ou professionnels. Malheureusement, contrairement aux mémoires numériques dont la capacité explose, celle des soignants a tendance à diminuer avec l'âge… Un logiciel doit donc permettre de saisir des notes personnelles, accessibles uniquement au soignant ou au médecin qui les rédige. Ces notes ne doivent pas être communicables aux autres soignants, ni au patient ou à ses ayant droits.

3. Non-respect, conscient ou non, de certaines réglés d'accès au dossier

Comme pour tous les professionnels de santé, bien que les règles d'accès soient largement diffusées et écrites, on constate parfois un élargissement des notions de secret partagé. Pour diminuer les clivages, accompagner des patients souvent déficitaires pour qu'ils puissent garder ou retrouver une place dans la société, il nous est habituel de partager leur histoire, leur problématique avec l'ensemble d'une équipe soignante, dont certains membres ne prendront pas toujours directement en

charge le patient, voire avec de précieux partenaires extérieurs (médecin traitant, famille, assistante sociale, équipe d'Ehpad ou de maintien à domicile, tuteur ou curateur…). Ne pas partager certains éléments avec ces personnes ressources pénaliserait le patient, entrainerait un risque social ou vital pour lui et il nous faut arbitrer quand cela est nécessaire, en recueillant le consentement du patient.

Les soins psychiatriques se déroulent souvent sur des lieux multiples, avec des équipes diverses, d'un ou plusieurs services (CMP, Hôpital de jour, addictologie, hospitalisation temps plein), avec des patients qui peuvent cliver les prises en charge,ce qui implique l'accès simple au dossier depuis ces différentes structures par les professionnels concernés et des observations claires et explicites. Un infirmier de nuit dans une unité pourra être appelé par un patient sorti 6 mois plus tôt et aura besoin de trouver dans le dossier les informations nécessaires pour le rassurer, l'orienter ou l'informer de sa prochaine consultation.
A l'inverse, cette notion extensive du secret partagé pourrait pousser à consulter des dossiers par curiosité. Pire, la confusion et le dysfonctionnement induits par certaines pathologies psychiatriques ou systèmes familiaux peuvent nous pousser à consulter d'autres dossiers de façon inadaptée. Dans une même affaire, nous pouvons être amenés à suivre auteur et victime de violences. Est-il légitime quand je vois une victime (ou présumée victime) d'agression ou d'emprise de vérifier sur l'agenda de ma collègue si l'agresseur ne vient pas en consultation ce jour-là en même temps qu'elle? La sollicitation pourra être grande, au vu de la description par un patient, de consulter un autre dossier pour vérifier si la personne est suivie, ou de confronter le discours de mon patient aux notes de l'autre dossier pour « démêler le vrai du faux » d'une situation confuse ou limite ? Les tentations, qui étaient minimes quand il fallait fouiller l'armoire à dossiers papiers, ne nécessitent plus que de petites manipulations informatiques, au fond d'un bureau isolé…

On voit qu'au départ, de bonnes intentions peuvent amener à un non-respect des règles d'accès au dossier, et que ce danger peut être démultiplié par la puissance de ces nouveaux outils. Imaginons alors le risque si je dispose d'un accès aux dossiers de toute la région…

4. Dysfonctionnements spécifiques à la psychiatrie

« Travailler avec des fous n'est pas sain » disait un de mes Professeurs. Effectivement, les dysfonctionnements liés à la psychose, aux perversions individuelles ou de systèmes (familiaux, professionnels, etc…) peuvent entraîner patients, soignants ou entourages dans des dérapages. Ainsi, un professionnel de santé a-t-il pu donner ses codes d'accès à un membre de sa famille pour qu'il consulte son propre dossier... et ait accès au diagnostic de schizophrénie, mais également aux contenus des observations et appels téléphoniques des professionnels. Le risque lié au fait de porter « la double casquette » (professionnel et entourage) peut être redoutable. Peut-on le baliser a priori ?

Les dossiers psychiatriques sont nécessairement riches d'informations concernant l'histoire du patient et de son entourage, d'échanges avec les équipes de professionnels, d'éléments décrivant d'autres professionnels, tout ceci participe à cette clinique. Nombre de diagnostics psychiatriques sont considérés comme des injures par les non professionnels, voire certains soignants. Une description d'un fonctionnement familial pourra être vécue comme porteuse de jugement, voire culpabilisante par les intéressés. Enfin, nos patients peuvent être dans le déni de leur maladie, interprétatifs ou persécutés.

5. In fine, quelles habilitations d'accès aux données médicales en psychiatrie ?

Soyons honnêtes, il n'existe pas de consensus dans la profession. Toutefois, il paraît préférable d'être prudent avant d'exposer des données très personnelles à des milliers voire dizaines de milliers de professionnels, si on ne veut pas s'exposer à de multiples violations du secret ou que les professionnels deviennent trop prudents et vident de leur substance les dossiers informatisés, proposition régulièrement avancée par certains collègues.

Il paraît utile de prévoir des droits d'accès limités a priori, que le dossier ne soit accessible intégralement qu'à tous les soignants du ou des services psychiatriques prenant en charge le patient (la création d'un acte de suivi entraine un accès automatique au dossier). En revanche, tous ces professionnels doivent pouvoir y accéder depuis les multiples lieux de soins et pas seulement depuis le site d'hospitalisation temps plein.

L'accès à tous les médecins du GHT pourrait se limiter aux antécédents somatiques, traitements médicamenteux, résultats paraffiniques. En revanche, tout médecin ou infirmier des services d'urgences devrait pouvoir bénéficier d'une fonction bris de glace permettant l'accès effectif à l'intégralité du dossier, avec message d'avertissement préalable et alerte du DIM avec traçage de l'accès au dossier qui permettra un contrôle a posteriori de la légitimité de cet accès. Bien sûr, une politique d'information des droits et de sanction des infractions est nécessaire si l'on veut que ces mesures soient efficaces.

Enfin, des notes personnelles accessibles au seul professionnel qui les rédige (médecin, psychologue, infirmier d'accueil)paraissent parfois utiles.

En revanche, le recours à un anonymat du dossier par un nom fictif, comme le proposent certains éditeurs de logiciel, nous parait, sauf exception, dangereux et source de perte d'information.

On voit donc qu'il existe une forte tension entre le besoin de transparence et d'accès rapide aux données médicales de plus en plus réclamée en médecine et les impératifs spécifiques à la psychiatrie. L'enjeu est donc très fort sur la politique d'habilitation d'accès aux données et oblige à faire du sur mesure…et ne peut totalement protéger de tous les risques de violation du secret médical.

6. TRACES D'ACCÈS ET CONTRÔLES DES TRACES

La confiance n'exclut pas le contrôle, et pour les pans du DPI qui sont en mode à posteriori, l'ouverture des droits a pour corollaire indispensable le contrôle, par le biais de l'analyse des traces générées par le DPI pour toute action réalisée par les utilisateurs : ouverture de session, consultation d'un dossier, création ou modification d'une donnée, etc.

6.1 Les bases du contrôle des traces

Le contrôle des traces doit comporter au moins trois aspects :

• possibilité d'interroger les traces par l'entrée « patient » : il doit être possible, pour un patient donné, de savoir qui a eu accès à son dossier, pour y faire quoi (lecture, écriture, consultation, etc.) et sur une période de temps choisie ;

• possibilité d'interroger les traces par l'entrée « utilisateur » : il doit être possible, pour un utilisateur donné (praticien, personnel soignant, personnel administratif, etc.) de savoir quels dossiers patients il a consulté, et pour y faire quoi, le tout sur une période de temps choisie ;

• requêtes paramétrées : il doit être possible de paramétrer des requêtes correspondantes à des cas d'usage que l'on sait être des anomalies ; par exemple la consultation par un professionnel de santé du dossier d'un patient qui n'est pas dans son service ou pôle ; ce corpus de requête doit pouvoir facilement évoluer, au fur et à mesure des nouveaux cas « suspects » que l'on rencontre ;

• traitement particulier des dossiers sensibles ou hyper confidentiels, ou du déclenchement du bris de glace ; les requêtes correspondantes à ces typologies spéciales doivent être pré-paramétrées dans l'outil ;

• enfin, dans l'idéal, un outil d'interrogation de la base des traces en mode multicritères : service, praticien, patient, dates, etc. ; et le tout avec un langage ensembliste évolué de type SQL ;

6.2 Le contrôle des traces au quotidien

Il est indispensable de définir en tout premier lieu les responsabilités : la DSI n'a pas vocation à effectuer ces contrôles, qui échoient en général au DIM ou à une cellule spécialisée. La DSI doit en revanche mettre à disposition les outils et en particulier écrire les requêtes les plus complexes.

Dans l'idéal, chaque mois une personne de l'équipe en charge des contrôles :

• lance chaque requête paramétrée afin d'en relever les anomalies, et les traite ; attention, les traces génèrent pas mal de faux positifs. Pour une anomalie détectée,

il n'est pas rare de devoir passer plusieurs heures à instruire ;

• procède à un contrôle par échantillonnage des traces de praticiens, personnels médicaux et personnels administratifs ;

• intègre les cas d'usages nouveaux en paramétrant de nouvelles requêtes - ou en demandant à la DSI de le faire si c'est trop technique.

Toujours idéalement, chaque année un rapport des anomalies et de leur évolution pluriannuelle devrait être rédigé.

Difficulté de traces des accès aux DP des agents qui sont en même temps des patients

Dans beaucoup d'établissements, une bonne partie des indiscrétions est due à la consultation, par les agents eux-mêmes, des dossiers médicaux de leurs collègues (qu'ils ne prennent pas en charge s'entend), pratique particulièrement détestable.

Il est tentant de positionner systématiquement tous les agents / patients en mode hyperconfidentiel, sauf que cela induit une perte de chance et de fait cette décision revient au patient et à lui seul.

De plus, cela nécessiterait de croiser l'annuaire des agents avec celui des patients, ce qui engendre d'autres problèmes au regard du RGPD : en tant que DPO je suis défavorable à ce croisement.

La seule solution est d'indiquer aux agents que leur propre DP pourra à leur demande être taggué « sensible » (ce qui suppose que le DPI intègre cette notion) sans que cela soit un statut d'hyperconfidentialité et que des requêtes d'analyse de traces spécifiques seront lancées sur ces dossiers en particulier. Ce sujet est cependant très complexe.

6.3 Les conditions réglementaires du contrôle

Il est utile de préciser que tout contrôle de l'utilisation du SI doit absolument être mentionnée explicitement dans le règlement intérieur, le plus souvent dans la Charte Utilisateur qui en est une annexe. Et pour être opposable, la charte en question doit être passée aux instances de l'établissement, selon un processus que les DRH maîtrisent en général très bien.

Exiger la signature d'une charte ne sert à rien

Cela n'a aucune valeur juridique. C'est très facile à contourner de la part des agents retords et en plus la logistique est très difficile à maintenir dans le temps. Économisez-vous du temps et de l'énergie : faites passer votre charte aux instances, et révisez-là environ tous les 5 ans.

6.4 Politique de sanction

Contrôler, constater des anomalies dans les accès (par exemple un personnel administratif qui est allé consulter le dossier médical d'un collègue par pure curiosité) et ne rien faire est le meilleur moyen de saper la confiance dans l'outil informatique.

Du reste, en cas de contrôle CNIL, si les auditeurs de l'autorité de régulation constataient l'absence de sanction suite à malveillance, la responsabilité civile et/ou pénale de l'institution pourrait être engagée.
Il est donc nécessaire d'avoir une politique de sanction, qui est du ressort de la DRH et d'elle seule. Et comme toute politique, elle doit être écrite (Plan), appliquée (Do), auditée (Check) et corrigée (Act).

6.5 Opposabilité des contrôles

C'est un sujet qui est étonnamment peu traité, et il est pourtant primordial. Supposons que l'analyse des traces d'accès au DPI révèle que l'agent X a consulté, sans aucune raison légitime, le DP de l'agent Y. Si vous entamez une procédure de sanction à l'encontre de l'agent X, vous devez savoir que ce dernier pourra vous opposer le fait que l'établissement s'est constitué une preuve pour soi-même, en l'occurrence des traces techniques. Et cela rend, dans beaucoup de cas, la trace en question non opposable.

Certes, au final, c'est toujours un juge qui décide si un élément de preuve produit par une des parties est valable ou pas, mais à partir du moment où les traces ne sont pas collectées selon un système qui en garantit l'intégrité technique, l'agent X pourra toujours affirmer que ce n'est pas lui mais un copain de l'informaticien qui est à l'origine de l'accès indu, et que l'informaticien en question est allé modifier les traces pour exonérer son copain. Ce n'est pas pour rien qu'HADOPI faisait collecter les traces par une tierce partie.

Si l'accès indu en question devait amener au licenciement de l'agent en question, les traces seules ne suffiraient pas et il faudra un dossier plus étayé.

DPI ET GESTION DES DROITS D'ACCÈS AUX DOSSIERS MÉDICAUX

Écrit par l'équipe Evolucare

Romain LE GUILCHER
DGA et directeur communciation

Nadou YEO
RSSI - DPO

Lân GUICHOT
Consultant

La question de la politique d'habilitation des accès au dossier médical d'un patient est un très vaste sujet. La réponse n'est pas simplement unique : de nombreux facteurs entrent en jeu du fait de la complexité des organisations et de la multitude des métiers impliqués. L'objectif ici, est de rappeler quelques fondamentaux et décrire certains usages rendus possibles avec des fonctions avancées créées par certains industriels éditeurs, dont EVOLUCARE. Ainsi, le lecteur pourra se poser ou se « re poser » les quelques questions, lui permettant de corriger, d'adapter sa politique de sécurité de son SI, Système d'information en perpétuelle mutation du fait des organisations changeantes mais aussi des évolutions des exigences réglementaires.

Ici ne sera pas abordée la gestion des droits d'accès techniques à travers une vision logicielle, mais plutôt une vision de l'habilitation à travers le cycle de vie de la donnée. En effet, les modalités de paramétrage technique des droits d'accès varient fortement selon la ressource concernée d'une part, et selon les outils utilisés pour la gestion de ces droits d'autre part.

1. Quelques évolutions plausibles

Aujourd'hui, le DPI est un vocable d'usage voulant signifier **D**ossier **P**atient **I**nformatisé. **Hier**, il a connu plusieurs vocables comme par exemple le **DMC**, pour **D**ossier **M**édical **C**ommun. Commun par opposition aux multiples dossiers de spécialités médicales qui ont eu leur heure de gloire et de nos jours en déclin du fait d'une inter opérabilité inexistante, voire impossible et pour certains pour leur caractère non industriel, dangereux pour la sécurité des patients.

En déclin ou disparition, les positions fortes de certains, comme bien résumées ici : «*Il est hors de question que je mette MES données de MES patients dans un logiciel que tout le monde pourra consulter*». De plus, ces dossiers de spécialités médicales possédaient une gestion des droits d'accès rudimentaires privilégiant une définition unitaire des habilitations du fait du nombre restreint d'utilisateurs. Les DPI ont mis en place une définition de profils d'habilitations plus adaptés aux grands nombres d'utilisateurs ayant des métiers différents et aux plus grandes organisations.

Ce DMC s'est voulu au départ MINIMUN commun (quelques documents de « bureautique médicale », comme par exemple l'anamnèse, le compte-rendu opératoire ou le compte-rendu d'hospitalisation). Puis progressivement il s'est transformé en un Dossier MAXIMUM commun, adressant tous les services d'un établissement et tous les acteurs de la chaine de prise en charge. Cela pose alors la question de comment sécuriser et partager un dossier devenu holistique de par son contenu mais aussi des fonctions de production et de consultation des données gérées. D'où l'importance d'une vision orientée « data ».

Et demain, quelle sera la nouvelle dénomination de ce DPI ? Un dossier Patient Longitudinal ? un Dossier Sociétal ? Un portail pour les professionnels, pour les patients ? Une Plateforme de services numériques ? …

En effet les pratiques et les usages ont évolué et continuent d'évoluer :

1. Les utilisateurs se transforment en usagers avec une notion de balance entre effort de contribution et bénéfices rendus.

2. Les organisations de soins au départ mono entité deviennent des multi entités, à l'image des GHT, des Groupes de cliniques, etc…

3. Les prises en charge évoluent vers une logique de parcours visant à faire disparaître les ruptures de prise en charge en faveur d'une logique de continuum de soins, transverse à un territoire.

4. La coordination induisant la collaboration des métiers oblige le partage de l'information produite par chacun.

5. Les usagers sont devenus des acteurs et veulent disposer de services, si possible organisés en bouquets.

6. La Data est devenue cruciale depuis l'avènement de l'Intelligence Artificielle, pour un professionnel ou un patient « augmenté ».

7. La quête incessante du « mieux » à défaut du « faire plus avec moins » pour le professionnel mais aussi finalement pour le patient.

8. Un patient qui est devenu un « patient /citoyen » car la logique territoriale induit la prise en compte du sanitaire mais aussi du médico-social, où il s'agit de considérer d'une part le patient et d'autre part le résident ou bien l'usager : bref une personne, un citoyen finalement.

9. Les étapes du parcours de soins ou de vie, donnent une place considérable à l'étape relative au secteur MÉDICO-SOCIAL, positionnant EVOLUCARE comme

incontournable, quand on connait les conséquences liées au vieillissement des populations. Les prises en charge deviennent en conséquence polypathologiques et nécessitent un partage d'informations souvent crucial à la sécurité des patients entre les différents épisodes de soins.

10. … / … (à vous cher lecteur de trouver le 10ème point et les points suivants …)

Cela étant dit, il est nécessaire avant de construire / adapter une politique de sécurité du système d'information médical, de bien identifier son réel contenu, avec une logique orientée « data », pour un SI « local » ou « étendu » (taille de l'organisation(s) et périmètre interne et/ou externe à l'entité(s) administrée(s)).

2. Quelques fondamentaux

Finalement, il est toujours question de prise en charge quelques soient les acteurs ou les lieux où se déroule ladite prise en charge pour des activités du secteur sanitaire ou bien de celui du médico-social.

Nota : Gardons cher lecteur, ce vocable DPI pour considérer toutes les prises en charge, celles des patients mais aussi celles des résidents et des usagers - elles auront pour objectif le meilleur soin, tandis que d'autres auront pour objectif une meilleure bientraitance.

La plupart des solutions « DPI » combinent deux entités pour que puisse se dérouler cette prise en charge :

1. Une entité de LIEU, on retrouvera ainsi la notion d'Unité d'HEBERGEMENT, concept qui est invariant quand on traite une hospitalisation ou un rendez-vous de consultation ou d'examen en présence du patient. Ce concept pourrait évoluer avec l'avènement de la virtualisation des pratiques avec la télémédecine, la téléconsultation ou la télé expertise induisant une notion de PARCOURS qui est finalement un ensemble de lieux physiques et/ou virtuels que l'on pourrait appeler ÉTAPE de prise en charge.

2. Une entité de RESPONSABILITÉ MÉDICALE, on retrouvera ainsi la notion d'Unité de RATTACHEMENT, concept invariant quand on choisit de paramétrer sa structure dans une stratégie orientée spécialité médicale ou personnalisée. A cela pourrait se rajouter la notion « d'ayant droit » pour considérer « l'équipe médicale » ou de délégation de droit pour considérer les jeunes professionnels en formation impliqués dans les prises en charge. Ce concept quant à lui pourrait demeurer.

Alors les principes de droits d'accès sur historique d'un DPI sont généralement les suivantes : (CF FIGURE 1)

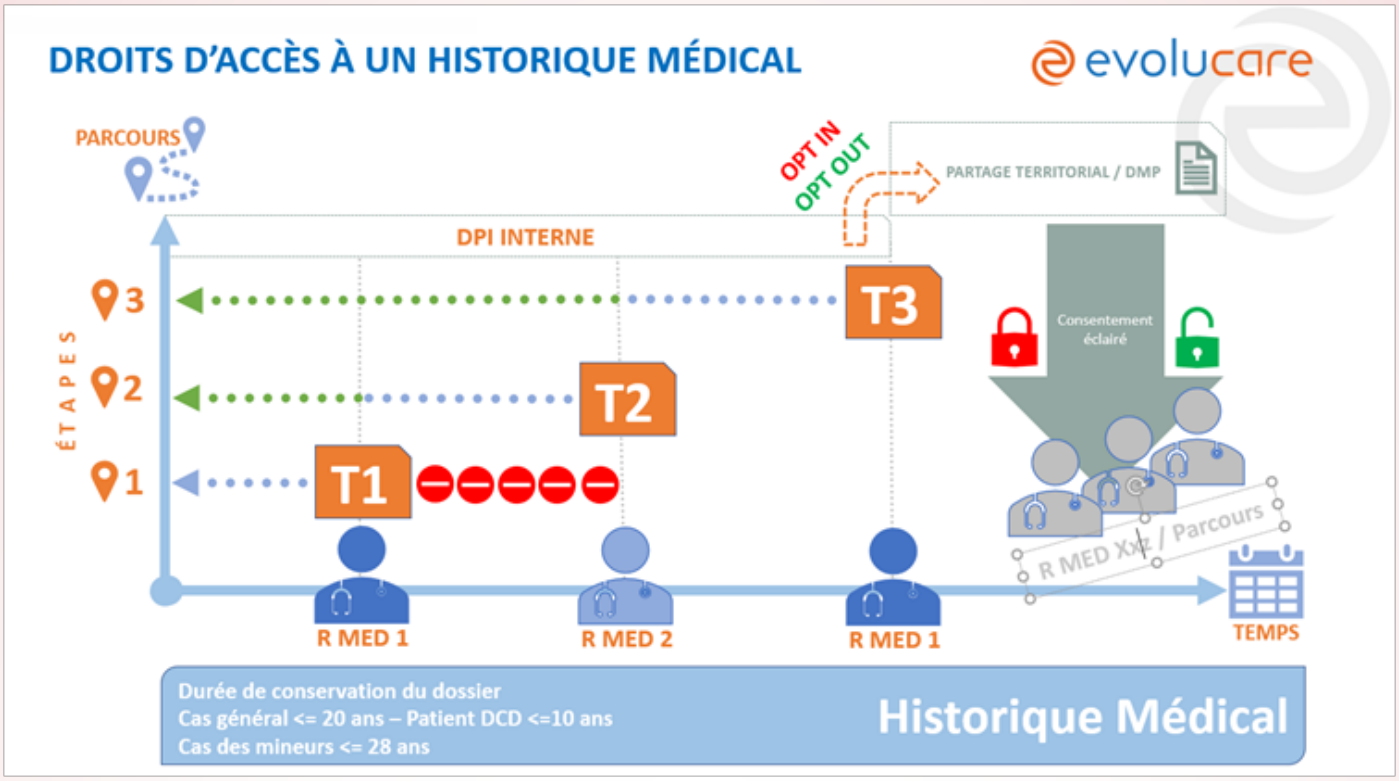


FIGURE 1

• A l'instant T1 - ÉTAPE 1

La responsabilité médicale 1 se verra ouvrir les accès à l'historique de l'instant T1 à moins l'infini, avec respect des nouvelles règles du RGPD relative à la durée de conservation des dossiers : pour le cas général, une profondeur de 20 ans, pour le cas des patients décédés, une profondeur de 10 ans, et pour les personnes mineures, une profondeur de 28 ans.

• A l'instant T2 - ÉTAPE 2

La responsabilité médicale 2 se verra ouvrir les accès à l'historique de l'instant T2 à moins l'infini, (avec respect des nouvelles règles du RGPD décrites plus haut). L'épisode T1 à moins l'infini lui, est donc accessible pour que sa responsabilité médicale puisse pleinement s'exercer. En revanche la responsabilité médicale 1 ne pourra pas accéder à l'épisode correspondant au temps T1 vers T2. Alors pour gérer l'arrivée tardive de résultats d'examens ou autres productions une notion de CLÔTURE vient verrouiller l'épisode quelques jours après le départ effectif du patient du lieu de la prise en charge.

• A l'instant T3 - ÉTAPE 3

Le patient est repris en charge par la responsabilité médicale 1. La responsabilité médicale 1 se verra ouvrir les accès à l'historique de l'instant T3 à moins l'infini, (avec respect des nouvelles règles du RGPD décrites plus haut). L'épisode T1+T2 lui est donc accessible pour que sa responsabilité médicale puisse pleinement s'exercer.

L'usage général est de ne lister que les patients physiquement présents dans un lieu de prise en charge donné. On parlera de VUE par HÉBERGEMENT, utile aux infirmiers qui ne peuvent voir que les seuls dossiers des patients physiquement présents dans leur unité d'hébergement.

En revanche, il faut pouvoir offrir aux médecins et leurs secrétaires une vue dite de

RATTACHEMENT permettant d'afficher les patients pris en charge sous une même responsabilité médicale quel que soit le lieu de prise en charge, que ce soit dans le même bâtiment, à un autre étage ou dans un autre pavillon. Ainsi ces vues, permettent la souplesse face aux débordements fréquents de patients d'un service à l'autre ou pour des établissements organisées en unités multi spécialités (multi-responsabilités médicales).

Par ailleurs, une certaine catégorie de professionnels sont appelés à être affectés à des unités d'hébergement en fonction des « suractivités », des plans blancs ou même des pandémies telle que celle que nous connaissons actuellement avec la COVID-19. Il s'agit de profils dit « VOLANTS », c'est le cas pour certaines secrétaires ou infirmières, mais aussi des responsables de garde, des médecins urgentistes ou DIM : doit-on leur ouvrir des habilitations pour toutes les vues de toute la structure de soins ? Bien évidemment, non, même avec une traçabilité et une journalisation complète des actions, tellement le risque de dérive pourrait être grand.

La réponse à cette problématique est possible avec une gestion des vues dépendantes du contexte géographique où le professionnel s'identifie et entre dans le SI médical. Pour cela la solution peut s'appuyer sur un identifiant unique du poste de travail, unique, mais très vulnérable au spoofing. Peut-être hasardeux d'en faire allusion dans un article sécurité et les vues à associer à ce lieu. Cela sous-entend une cartographie et un plan de maintenance précis en cas de remplacement des stations. Ainsi les vues changent automatiquement lors des déplacements de ces professionnels avec prise en compte des habilitations attachées aux hébergements et responsabilités médicales décrits plus haut. Pour les postes de travail mobiles, des solutions de maillage de réseaux existent tout autant que la technologie par exemple de types BEACON ouvrant le champ des possibles pour une expérience utilisateurs plus interactive et plus contextuelle. (Chers éditeurs : à vos claviers …)

Les profils d'habilitation sont établis avec des fonctions unitaires sujettes à droit, dont une traçabilité doit être mise en œuvre. Les profils ainsi crées tiennent compte en général des métiers qui eux-mêmes sont définis par des droits, des devoirs et des responsabilités. (Cf Services RH et autres contrats de collaboration)

3. Consentement éclairé

Voici une disposition qui a été plus une contrainte qu'une évolution sur la sécurité relative aux données médicales des patients et qui a été un véritable frein à tous les projets visant à faire avancer le numérique en santé, dans l'axe des échanges et partages, au service tout simplement des professionnels et de leurs patients. La non-complétude du DMP en est une preuve. Cela concerne aussi d'autres projets de dimension plus régionale ou territoriale. Si bien qu'un dispositif OPT IN et OPT OUT est en passe d'être généralisé.

La Loi OTSS qui prévoit l'ouverture d'un dossier DMP par défaut avec la possibilité pour l'usager de la refuser (OPT-OUT) peut constituer un premier élément juridique nous permettant une approche rationnelle et juridiquement pertinente. Il faut pour cela que le patient ait la possibilité non seulement de s'opposer au partage de ses informations, mais également d'accepter qu'un professionnel donné puisse - dans son intérêt - accéder à l'information pour la partager, si le patient le souhaite et lui donne son accord explicite. Ceci implique au moins l'export de son identité vers la solution territoriale pour que son médecin puisse acter sa volonté de partage. En l'absence de cette identité, l'expression de son accord devient impossible si l'information ne lui a pas été donnée au sein du système d'information dans lequel a eu lieu la prise en charge, du fait d'une méconnaissance de l'importance de cette information par le médecin hospitalier qui a alimenté son dossier médical (ou pire, d'une négligence…).

OPT-IN est la procédure déjà connue nécessitant une consentement éclairé préalable et explicite.

Et si le non-partage « d'emblée » de l'information pouvait être considéré comme une « **perte de chance pour le patient** » ? Quand on sait qu'en général seulement 2% des patients expriment leur volonté de ne pas partager voire de supprimer leurs données, une solution serait de modifier les procédures de consentement actuelles (OPT-IN) avec description du caractère « étendu » du SI dans lequel la personne est prise en charge.

4. Quelques dérives possibles

Dans la logique évènementielle décrite plus haut, il suffit par exemple tout simplement à un utilisateur possédant les droits, de créer un événement de type HOSPITALISATION ou RDV pour consulter le dossier d'un patient, alors que ce dernier n'est pas présent. Une fois la consultation ou l'édition réalisée, il suffit de supprimer l'évènement et le tour frauduleux est joué… La traçabilité et la journalisation sont là pour éviter ces dérives.

Ces dérives peuvent survenir et devenir finalement quotidiennes. Leur nombre semble être lié au caractère « fermé » ou « plus ouvert » de la stratégie de gestion des habilitations.

La politique fermée « à priori » basée sur une matrice de droits binaires « ouvert » / « fermé » ne semble pas adaptée aux organisations complexes. En effet le nombre d'exceptions à gérer prend le pas sur la gestion des cas généraux. Ainsi la dérive observée est celle du « bris de glace » utilisé trop systématiquement, certes tracé et documenté, mais dont les journaux ne sont pas ou très peu exploités. La forte tentation d'utiliser des identifiants génériques augmente les dérives. Ces derniers se prêtent et le résultat est peu enviable, a vrai dire, pas viable du tout. Les indiscrétions ne sont, dans la plupart des cas, pas détectées, ni détectables facilement.

Les accès au DPI doivent donc être tracés dans des journaux requêtables périodiquement, en particulier pour des actions jugées sensibles. Selon les recommandations de la CNIL, les utilisateurs du Système d'Information en sont avertis et l'ont validé en signant la charte de la confidentialité, d'utilisation des TIC, et de la Sécurité du Système d'information, à la connexion au SI. Afin de ne pas bloquer les utilisateurs dans leur pratique et leur permettre d'accéder à toutes les données qui pourraient être utiles dans la prise en charge des patients, une politique d'habilitations « plus ouverte » peut être mise en œuvre, mais avec un vrai contrôle « à postériori ». La porte ouverte aux accès réellement illégitimes doit être assumée. Même si en termes juridiques le « préjudice est constitué », ces accès sont faits en toute connaissance de cause de la part de l'utilisateur, qui a été averti et a validé ces accès hors délégation. Si, après interrogation de l'utilisateur, ces accès sont réellement illégitimes (réalisés hors d'un contexte de soin), il convient d'en sanctionner l'auteur, en rendant opposable le fait qu'il en ait été averti.

5. Finalement

Les solutions territoriales mise en œuvre respectent-elles toutes ces logiques fondamentales d'accès aux historiques médicaux ?

Chers GHT(s) : Remplacer les DPI par un DPI unique est-il vraiment la seule solution, quand on connait les énormes investissements financiers et humains nécessaires à leur mise en œuvre et la politique de sécurité d'accès propre à la stratégie de chacun des établissements ? Ces derniers restent encore des entités juridiques à part entière, ce qui pose également la problématique de la convergence des politiques de sécurité des SI ?
Et si la convergence tant désirée était considérée avec plutôt, un axe de convergence des données ? En effet, « les GHT ont été créés par DÉCRET… mais cette convergence induisant la nécessaire coopération se DÉCRÈTE-t- elle ? » Telle est la question que nous devons nous poser…

Les équipes expertes du groupe EVOLUCARE sont à votre écoute pour répondre à ces questions.

EVOLUCARE
www.evolucare.com
contact@evolucare.com
03.22.50.37.90

7. Le lien avec un IAM

Une brique IAM (Identity Access Management) réalise plusieurs fonctions, et notamment la création plus ou moins automatisée des ID/MDP applicatifs à partir de sources fiables d'identités, telle la gestion RH. A priori, cela dispense de la création manuelle des ID/MDP dans les progiciels métier, notamment le DPI. Il y a cependant plusieurs bémols et contraintes.

7.1 Les conditions du provisionning fin

D'une part, la seule connaissance de l'identité physique de la personne ne suffit pas pour mettre en place un provisionning automatisé des ID/MDP et des habilitations. Il va falloir disposer également d'informations précises permettant de calculer les profils et les rôles : métier, grade, diplôme, service d'affectation, etc. Plus on voudra aller loin dans le provisionning, plus ces informations devront être connues de façon précise, ce qui n'est pas simple sur le strict plan RH, pour des raisons évoquées plus haut.

7.2 La question des habilitations

Même en disposant d'informations précises sur les agents, l'expérience montre que, si le provisionning automatique d'identité est assez facile à mettre en œuvre, le provisionning des habilitations n'est efficace que tant que l'on reste au niveau macroscopique : dès que l'on va toucher des profils complexes ou transversaux, l'attribution d'habilitations fines ne pourra être réalisée que manuellement.

Ceci a deux conséquences : d'une part il faut disposer d'une matrice des droits fins à jour. Pour élément de comparaison, dans un CHU, quand cette matrice existe, elle comporte des dizaines de colonnes (les profils) et plus de 100 lignes (les droits fins). Cela représente donc une charge de travail conséquente, en constitution et en maintenance.

D'autre part, quelle que soit l'exhaustivité de cette matrice il faudra gérer des exceptions, et on retombe sur la question de la responsabilité de décider ce qui est ou pas une exception. La réponse ne peut passer que par l'identification d'une MOA officielle, et surtout de la stricte séparation des rôles entre la MOA qui décide et la MOE qui exécute.

7.3 Les audits d'écart

Aucune brique IAM n'est parfaite et au fil du temps, on constate forcément des dérives : il est indispensable de mettre en œuvre des audits d'écart pour identifier ces dérives, aussi bien des glissements de droits que des profils orphelins, des profils manifestement « surdimensionnés » en termes d'habilitation, des agents ayant quitté l'établissement mais dont les ID/MDP sont toujours actifs (l'IAM est un logiciel, et tout logiciel a des bugs), etc.

8. Les outils techniques de réponse aux besoins de confidentialité

Dans certains cas, le critère de confidentialité est prépondérant et il peut être nécessaire de mettre en œuvre des mécanismes techniques en sus des habilitations.

8.1 Anonymat et pseudonymat

Stricto sensu, anonymiser une donnée revient à rendre impossible l'identification de la personne concernée par ces données (patient, client, agent, etc.), alors que la pseudonymisation revient à remplacer l'identité par un code, la correspondance identité-code étant confiée à une autre entité que celle qui traite techniquement les données. Dans le cas de la pseudonymisation, il est donc techniquement possible de remonter à la personne.

Premier bémol : selon les derniers résultats de recherche dans le domaine, il n'est pas possible d'anonymiser totalement une donnée. En croisant une donnée anonymisée avec d'autres sources de données nominatives, il a été démontré que dans de nombreux cas il était possible de remonter à la personne. La position de la CNIL concernant l'anonymisation est de considérer qu'une donnée est anonyme dès lors que les moyens mis en œuvre pour remonter à la personne sont disproportionnés (au sens technique et financier).
Deuxième bémol : il y a des données qu'il n'est pas possible d'anonymiser, par exemple les données génétiques.

Il existe cependant des outils qui permettent d'atteindre un excellent taux d'anonymisation : par exemple la technique des avatars de la société WEDATA (voir à ce sujet cet article dans DSIH).

Ce sujet occuperait un opus à lui seul et dépasse largement le cadre de cette publication. Il faut simplement retenir que :

- anonymiser n'est jamais facile, et le fait de ne conserver que les initiales des noms et prénoms n'est absolument pas une anonymisation ;

- anonymiser ou pseudonymiser ne constituent pas une fin en soi, mais sont une réponse à un besoin et doivent être vus comme une mesure technique, parmi d'autres possibles, permettant de sécuriser des données.

8.2 Le chiffrement des données

Le chiffrement des données constitue une mesure technique permettant d'augmenter le critère de confidentialité, mais il s'agit globalement d'un trompe-l'œil.

La plupart du temps, les demandes de chiffrement des données métier stockées sur les serveurs ont pour objectif de prévenir l'accès à ces données par les informaticiens. C'est techniquement faisable mais en pratique très complexe à mettre en œuvre car cela suppose une gestion des clés de chiffrement par un tiers, ce qui dégrade de facto les possibilités d'intervention des informaticiens dans des cas classiques tel un problème sur un dossier en particulier, le fait de reproduire une cinématique d'écran, etc.

En revanche, le chiffrement des données en bas niveau (par le firmware directement) est une très bonne protection contre le vol physique de matériel. C'est d'ailleurs une mesure préconisée par l'ANSSI concernant les PC portables (qui se perdent dans les taxis, se volent dans les trains, etc.).

A la question « faut-il chiffrer les données métier », la réponse n'est pas oui ou non, mais « quel est le besoin ? ».

9. Les usages aux limites du modèle

Il existe certains besoins d'accès à une donnée métier - ici, médicale - qui tendent à échapper aux modèles classiques (à priori ou à postériori) qui tous implémentent le paradigme de « l'accès est réservé à celui qui prend en charge le patient ».

9.1 La recherche médicale

Le domaine de la recherche médicale est un champ bien à part, qui dépasse très largement le cadre de cet opus. D'autant qu'elle n'est pas monolithique : la recherche académique (recrutement de volontaire, protocole en double aveugle, etc.), la recherche clinique, les thèses et la recherche qui n'en n'est pas vraiment une au sens administratif (pas d'encadrement). La seule règle est : toute demande d'accès à une donnée médicale au motif de recherche doit suivre le circuit administratif ad hoc - dossier, autorisation, comité d'éthique, etc.

9.2 L'amélioration des pratiques professionnelles

Il s'agit d'un usage qui se déploie rapidement, avec un temps de retard sur l'informatisation des processus métier. En l'occurrence, il s'agit d'exploiter les données pour améliorer les façons de travailler.

Par exemple, côté RH, il pourrait s'agir de mesurer les temps de traitement de tel ou tel dossier (recrutement, contentieux, etc.) afin de voir si des agents du service RH ont besoin d'un accompagnement ou d'une formation aux outils informatiques.

La frontière

La frontière est mince, entre l'analyse des actions d'un agent sur un logiciel pour détecter le besoin de formation, et le flicage. Le DPO doit être très prudent.

Mais on le voit plus particulièrement dans le domaine du soin : la remontée obligatoire de certains indicateurs qualité (IPAQSS) sur la complétude des dossiers patient, la prise en charge de la douleur, etc., imposent d'analyser des données dans un autre objectif que le soin immédiat, même si le soin est supposé en bénéficier.

Quel type d'accès, accordé à qui (DIM, etc.) ou à quoi (programme), pourra-t-on remonter ultérieurement d'une information agrégée (le nombre d'agents de tel service qui génèrent plus d'erreur que la moyenne) aux personnes nommées (pour les contacter et les accompagner), quel encadrement RGPD… : autant de questions qui rendent ce sujet complexe.

9.3 L'analyse des données pour les optimisations organisationnelles

Ce cas pose moins de problèmes que le précédent, mais il tend à se développer : il s'agit d'analyser les données d'activité d'un service sur une période déterminée (mois, trimestre, année) afin de prévoir les dispositifs logistiques ou back office selon les pics d'activité.

Par exemple, si un service de traumatologie constate que, pour ce qui concerne les motifs d'admission, le week-end ce sont plutôt des accidents de la route et le mercredi plutôt des fractures, il va prévoir plus de plâtre le mercredi et plus d'appareils lourds le week-end (et c'est bien un exemple).

Cela nécessite d'accéder à des données patient, mais au contraire de l'exemple précédent, il n'y a pas besoin de remonter aux personnes. Cela étant il s'agit d'un traitement, et il doit être encadré.

10. Les problématiques connexes

10.1 Le cas des accès des informaticiens

Les personnels de la DSI ne disposent pas du droit d'en connaître concernant des informations métier, au sens de leur fonction au sein dudit processus métier : en tant que RSSI, je n'ai pas et je n'ai pas à avoir accès à des informations médicales, RH, etc.

Mais les contraintes de maintien en condition opérationnelle des SI font que, de facto, les informaticiens ont souvent des accès aux données, si ce n'est pas par l'applicatif lui-même, au moins par les couches techniques telle la DB, l'OS, etc. Et dans les faits, il est même rare que les informaticiens ne disposent pas de ID/MDP applicatifs, qui plus est avec des privilèges très larges, car il faut pouvoir débloquer un dossier, débugguer, créer ou supprimer des comptes, etc.

Il est très difficile de faire en sorte que les informaticiens ne puissent pas voir les données métier ni même les modifier. Des systèmes existent, mais ils sont très coûteux, pas tant sur le plan matériel ou logiciel que sur le plan organisationnel : chaîne de décision pilotée par la MOA avec présence 365-24, ID/MDP sous séquestre avec une procédure de révélation, etc. A titre personnel, je n'ai jamais vu de tels dispositifs mis en œuvre dans le monde de la santé.

Même les commissaires aux comptes, pourtant très pointilleux dès lors qu'un individu dispose du privilège technique pour modifier lui-même son propre bulletin de salaire, ne vont pas jusqu'à demander la suppression de ces types d'accès, mais exigent plutôt leur contrôle, leur audit, la suppression des accès non-strictement nécessaire ou attribués à des informaticiens ayant quitté la structure, etc.

Force est d'ailleurs de constater que les « manquements aux obligations de secret » imputables aux informaticiens eux-mêmes sont rares : toujours à titre personnel, en deux décennies de vie professionnelle, je ne l'ai constaté que deux fois sur plusieurs milliers d'informaticiens rencontrés.

Il est cependant nécessaire de revenir aux fondamentaux sur ce sujet : les ID/MDP à privilèges doivent être strictement limités aux seuls usages nécessaires, être nominatifs et auditables, et les traces générées par leur utilisation doivent être collectées et isolées du reste du SI (ce qui n'est pas trivial), etc.

10.2 Les habilitations d'accès aux données archivées

Les archives de données métier peuvent exister sous format papier ou dématérialisé. Pour les données médicales, compte tenu des historiques de chaque établissement de santé, il y a forcément un historique papier très important, qui peut se compter en kilomètres de rayonnages pour un CHU.

Quel que soit leur format, la question des habilitations aux données archivées se pose de la même manière que pour les données « vivantes ». Les trois modèles précédemment décrits s'appliquent totalement, et donc il n'y a pas, de ce point de vue, de difficulté additionnelle.
Il faut tout de même signaler que le « temps » des archivistes n'est pas le même que celui des « personnels sur le terrain » : les seconds parlent en mois ou en années lorsque l'on évoque la question de la fenêtre temporelle de visibilité de la donnée, alors que les premiers parlent en décennies voire plus.

Il faut être conscient que tout système de calcul d'habilitations (à priori ou à posteriori) est basé, d'une manière ou d'une autre, sur la présence d'un patient dans une unité de soins et la spécialité médicale du professionnel. Or, ces éléments ne sont pas stables sur une longue période : les spécialités évoluent, se scindent et se recomposent, des unités ferment, d'autres sont ouvertes, etc. En d'autres termes, les éléments de calcul de droits d'il y a 50 ans ont souvent disparu de nos jours.

10.3 Les requêtes judiciaires

La seule précaution à prendre, lorsqu'il s'agit d'accéder à une donnée médicale dans le cadre d'un contentieux, est la nécessité d'une requête formalisée : commission rogatoire ou équivalent.

Sans ce document, qui protège aussi bien le demandeur que l'établissement de santé, un dossier médical n'a pas à être transmis. Pas plus du reste qu'une donnée RH : il y a des questions qui reviennent régulièrement sur les forums concernant les pratiques quelquefois douteuses des organismes de recouvrement de créances, qui usent et abusent d'arguments à la limite de la malhonnêteté pour savoir si telle personne est bien salariée de tel établissement, obtenir son adresse, son RIB, etc.

10.4 Le droit d'accès aux données des personnes

La question est la suivante : les données d'une personnes stockées en base et opérées dans le cadre d'un traitement conforme (RH, santé, etc.) appartiennent à la personne en question, qui peut exercer un droit d'accès et de rectification (dans certaines limites, notamment pour les données de santé pour lesquelles le patient n'est pas stricto sensu propriétaire mais dispose tout de même de certains droits, certes limités).

Mais la trace d'accès du médecin X au DPI du patient Y relève de quel statut ? Est-ce une donnée relative au patient Y (qui peut alors légitimement demander qu'on la lui transmette), ou est-ce une donnée du médecin X (auquel cas le patient Y n'y a pas accès, sauf cas de réquisition judiciaire tel qu'évoqué ci-dessus) ?

La position de la CNIL a été assez changeante, au moins un temps, sur le sujet. Il semble que la doctrine soit maintenant de considérer que la trace d'accès est une donnée personnelle de la personne qui en est à l'origine (l'utilisateur du logiciel) et ne soit pas communicable à la personne dont les données sont traitées (patient, agent) en dehors d'une procédure judiciaire formelle.

SÉCURISER LE DPI, UN ENJEU PRIORITAIRE DANS LE SECTEUR DE LA SANTÉ

Par Loïc GUÉZO, Directeur Stratégie Cybersécurité EMEA au sein de Proofpoint.

Fer de lance d'une transformation en profondeur de notre système de santé français, le Dossier Patient Informatisé (DPI) se généralise aujourd'hui progressivement pour remplacer le traditionnel dossier médical papier, qui, mal structuré, souvent mal classé voire illisible, a plus que largement atteint ses limites.
Avec le DPI, c'est tout un secteur qui se numérise, sous l'impulsion notamment de Ma Santé 2022, réforme du système de santé annoncée par Emmanuel Macron en septembre 2018, qui se concrétise le 26 juillet 2019 par l'adoption de la loi relative à l'organisation et à la transformation du système de santé soutenue par la ministre de la santé Agnès Buzyn.

Cette révolution du secteur porte de nombreuses promesses, notamment en termes d'informatisation du processus de soin et de développement de technologies interopérables, censées connecter les patients, les soignants, les cabinets médicaux et même les appareils à usage médical, pour améliorer in fine l'efficacité de la prise en charge des patients.

1. Des données trop sensibles pour être volées

Si la numérisation offre de formidables opportunités, elle génère de nouveaux défis dans l'écosystème des soins de santé, notamment en matière de cybersécurité. En tant que véritable carnet de santé numérique au cœur de la chaîne de soin, le DPI conserve toutes nos informations de santé, traitements, résultats d'examens, allergies et permet un partage avec les professionnels de santé qui en ont besoin pour nous soigner.

Et ces données sont très précieuses. Contrairement à des données financières (comme un numéro de carte de crédit) qui peuvent être modifiées en cas de fraude, les données relatives à un patient définissent ce qu'il est (son numéro de sécurité sociale, son adresse, sa taille, son poids, les informations médicales le concernant voire sur son conjoint ou sa famille) et ne peuvent être remplacées. En cas de vol, l'individu se retrouve ainsi directement exposé, avec des conséquences variables allant de la perte de confidentialité, au chantage, à l'usurpation d'identité voire à la mise en danger physique.

Il existe également dans les données de santé une véritable dimension prévisionnelle qui apparaît inquiétante, puisqu'il serait possible en appliquant des algorithmes à ces données, de « caractériser » les patients et par exemple, de calculer la probabilité

de développer une pathologie, ou encore de s'en servir pour étudierle potentiel médico-commercial d'un traitement. Ces données sont donc une mine d'or pour les cybercriminels, qui tentent par tous les moyens de les dérober pour les monétiser.

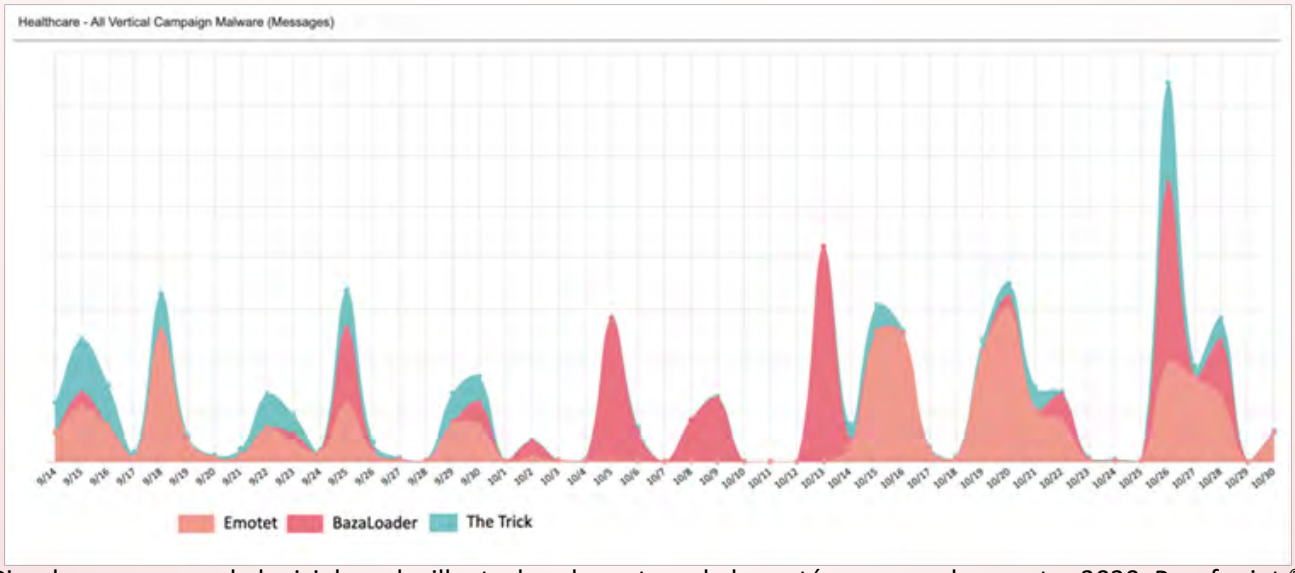
2. Tout un secteur déjà en danger

Si les cybermenaces évoluent, le fait que le secteur de la santé soit en danger n'est pas vraiment nouveau. Des masses de données précieuses et sensibles, un besoin souvent impératif de continuité de service et un patchwork d'infrastructures et de systèmes existants font de ce secteur une cible de choix pour les cybercriminelsdepuis déjà plusieurs années.

Que ce soit par le biais du phishing, de la compromission d'emails professionnels, de rançongiciels ou de toute autre forme d'attaque, les acteurs de la menace contournent les défenses des établissements de soins de santé pour accéder à des données personnelles, demander des rançons, et perturber les infrastructures médicales.

Et le pire reste encore à venir. En octobre 2020, le *FBI* a averti les hôpitaux et les prestataires de soins de santé américains de s'attendre à une « menace de cybercriminalité accrue et imminente, entraînant des attaques de rançongiciel, des vols de données et la perturbation des services de santé ». Fin novembre dernier, en plein confinement, l'agence nationale de la sécurité des systèmes d'information (ANSSI) lui a emboîté le pas et a dévoilé un *nouveau rapport* détaillant les caractéristiques techniques du rançongiciel Ryuk, une cybermenace particulièrement virulente et lucrative qui circule à travers le monde.

Le rapport de l'ANSSI précise qu'en octobre 2020, Ryuk a été responsable de 75 % des attaques sur le secteur de la santé dans le monde.La menace s'exporte et s'intensifie. Il semble donc important de mettre spécifiquement en garde les acteurs de la santé sur le territoire français.



Pics de campagnes de logiciels malveillants dans le secteur de la santé, au second semestre 2020. Proofpoint ®

3. Engager une réflexion sur la résilience du DPI

Face à cette cybermenace qui s'intensifie, le secteur doit être mieux armé pour détecter rapidement les attaques et les déjouer. En ce qui concerne le DPI, il ne faudrait pas qu'une fuite de données vienne remettre en cause son essence même… Il est donc primordial d'améliorer la sécurité des informations et la résilience pour prévenir les perturbations qui pourraient avoir un impact plus important sur la sécurité des patients.

Pour accompagner un système de santé en pleine mutation, le ministère des solidarités et de la santé a déjà mis en place le 1er octobre 2017 un dispositif de traitement des signalements des incidents de sécurité des systèmes d'information (SSI) des structures de santé. Avec l'Agence du Numérique en Santé, il apporte un appui aux ARS et aux structures concernées (les établissements de santé, les laboratoires de biologies et les centres de radiothérapies), au travers d'une structure nationale d'assistance et d'appui appelée « *Cellule Accompagnement Cybersécurité des Structures de Santé* » (ACSS). En deux ans, près de 700 incidents ont été déclarés via ce dispositif, un chiffre sans doute faible par rapport à la réalité, les victimes de cyberattaques préférant souvent se taire par crainte d'être stigmatisées, malgré les obligations légales de se déclarer.

Comme le prochain service national de cybersurveillance en santé, ce genre d'initiative est primordial pour non seulement accélérer le virage numérique en santé mais surtout améliorer le niveau de sécurité numérique du secteur.

4. L'email, premier vecteur d'attaque

La feuille de route du numérique dans la santé est encore longue. A côté du dossier patient, il y a aussi le point des messageries sécurisées de santé (MSS) pour sécuriser l'échange d'information de santé entre professionnels.

Si l'utilisation d'une MSS protégeant les données médicales des patients est une obligation légale en France, tous les établissements de santé ne l'ont pas encore intégralement déployée et le recours à des systèmes de messagerie plus traditionnels, hors contexte MSS, reste incontournable.

L'email étant aujourd'hui le principal vecteur d'infection, il est temps de porter une attention plus spécifique à ce canal de communication et de partage de données. Les acteurs de la santé peuvent se sentir protégés avec une messagerie sécurisée de santé de type MSS, mais en réalité ce n'est clairement pas le cas. En outre, ce type de système ne permet pas de donner une visibilité suffisante sur le réel niveau d'exposition aux cybermenaces, comme les rançongiciels. Il est donc urgent d'agir pour protéger un secteur déjà sous tensions dans un contexte sanitaire particulièrement éprouvant.

5. Une cyberdéfense centrée sur l'humain

Avec une image claire du paysage d'attaque, il devient possible d'adapter ses défenses pour tenir les acteurs de la menace à distance. Cela passe par la mise en œuvre d'outils de filtrage du courrier électronique pour arrêter les menaces avant qu'elles n'atteignent la boîte de réception et la création de processus de vérification pour limiter les chances de réussite des attaques d'usurpation d'identité et de compromission de compte.

Mais la technologie seule ne suffit pas. Les cyberattaques ciblent de plus en plus les personnes, et c'est donc l'humain qui constitue la ligne de défense la plus solide. Pour élaborer une stratégie de sécurité centrée sur les personnes, il faut d'abord identifier les personnes les plus attaquées au sein de la structure (Very Attacked People, VAP), et leur fournir les outils et informations nécessaires.

Cela commence par une formation de sensibilisation à la sécurité, couvrant les dernières menaces, méthodes et motivationscybercriminelles. Outre la capacité à repérer les liens malveillants et les courriers électroniques suspects, les utilisateurs finaux doivent comprendre que la cybersécurité est la responsabilité de chacun.

Pour que la protection soit efficace, il faut que la sensibilisation soit continue, approfondie et contextualisée. Des exercices de simulation de crise sont également de précieuses armes pour se préparer à lutter contre la menace et enclencher cette résilience dont le secteur a besoin. La menace étant en perpétuelle évolution, et les attaquants imaginant sans cesse de nouveaux moyens de contourner les systèmes de défense, le chantier de la sécurisation des systèmes d'information de santé doit être permanent.

Pour acquérir une visibilité sur les attaques de rançongiciel:
https://www.proofpoint.com/us/blog/threat-protection/providing-healthcare-organizations-visibility-latest-ransomware-attacks

Pour découvrir les tendances du paysage de la menace dans le secteur de la santé :
https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-fr-tr-healthcare-report.pdf

PROOFPOINT
www.proofpoint.com/fr
info-france@proofpoint.com
+33 (0)1 70 77 82 71

11. SPÉCIFICATIONS TECHNIQUES POUR LA GESTION DES HABILITATIONS D'UN DPI

Au regard de la question des habilitations, les éléments se classent en deux familles : les éléments qui concernent la gestion des habilitations à proprement parler, et les éléments qui concernent la gestion et l'exploitation des traces.

Le lecteur trouvera ci-après une liste, forcément non exhaustive, des spécifications à instruire. Il s'agit de pistes de réflexion, d'un guide à adapter au contexte (taille d'établissement, activité, etc.) : certaines peuvent être pertinentes dans un contexte et pas dans un autre, il convient donc de les adapter et cette liste n'a aucune prétention à constituer un cahier des charges exhaustif et/ou pertinent pour tous les cas d'usage.

11.1 La gestion des habilitations

[HAB01] : la matrice de relation rôle / unité doit pouvoir être implémentée en mode exclusif (un rôle a accès à toutes les unités sauf…) ou inclusif (un rôle n'a accès qu'à certaines unités). Attention cependant, ce mode peut rapidement induire une complexité difficile à maintenir dans la politique globale, mais l'objectif est de pouvoir positionner des unités en mode « à posteriori » et d'autres en mode « à priori ».

[HAB02] : il est nécessaire d'implémenter au moins deux notions : « patient sensible » et « séjour en hyperconfidentialité ». La différence entre ces notions doit être décidée par l'établissement, mais grossièrement « sensible » correspond à une alerte sans pour autant brider les accès, pour les admissionnistes ou les secrétariats, par exemple, qui doivent savoir qu'il ne faut pas donner d'informations par téléphone sur ces patients (prisonniers, victimes de violences conjugales, etc.) ; à contrario, la notion d'hyperconfidentialité entraîne un blocage d'accès à une information (séjour) et au masquage même de l'existence de cette information ;

[HAB03] : l'articulation entre l'hyper-confidentialité d'un séjour, et les unités à contrôle à priori, doit faire l'objet d'une réflexion poussée. Par exemple, un praticien d'une unité « à postériori » doit pouvoir accéder à certaines données des séjours d'une unité « à priori » (prescriptions médicales, etc.), mais l'accès à des données de séjours hyperconfidentiels doit se faire par un mécanisme de bris de glace. Une autre solution est de ne pas implémenter de mode de contrôle « à priori » mais de mettre les unités en question sous statut systématique d'hyperconfidentialité, en implémentant les mécanismes décrits en [HAB05]. Cette question est majeure pour les 10 prochaines années ;

[HAB04] : toute protection (patient sensible ou séjour en hyper confidentialité) doit être débrayable (bris de glace) avec des mécanismes d'alertes et de traçabilité appropriés.

[HAB05] : lors de l'accès au dossier médical d'un patient, le professionnel doit être alerté de la présence de données (séjour ou unité) hyperconfidentielles sans en voir

la liste. Il doit exister un premier niveau de bris de glace pour avoir accès à cette liste de données, et un second niveau de bris de glace pour voir les données à proprement parler. Ces deux bris de glaces doivent être auditables par des requêtes spécifiques et appropriées ;

[HAB06] : un dossier patient doit comporter un onglet qui liste tous les professionnels qui y ont accédé et pour quel motif (lecture, écriture, etc.), ceci afin que tout professionnel de santé sache qui s'est précédemment connecté au dossier du patient qu'il prend en charge. Idéalement il faut distinguer les accès par le personnel médical et soignant, des accès par les personnels « autres » (administratifs, Qualité, etc.) ;

[HAB07] : pour certaines spécialités, ou séjours, ou unités, le DPI doit permette aux professionnels de saisir des notes personnelles, visibles uniquement par le professionnel qui les a créées ;

[HAB08] : il doit exister un mécanisme permettant un accès « intuitu personae », par exemple pour les internes qui ont besoin d'avoir accès à une liste déterminée de séjours pour leurs thèses, les qualiticiens pour les indicateurs iPAQSS ou les juristes pour les dossiers de contentieux ;

11.2 La gestion des traces

[TRA01] : le module de gestion des traces doit proposer par défaut une requête sur les activations du mode bris de glace.

[TRA02] : l'analyse des traces doit pouvoir distinguer les accès pour motif administratif (facturation, etc.) et les accès pour motif de prise en charge médicale, ceci afin d'éviter le côté verbeux des traces.

[TRA03] : le module d'analyse des traces doit proposer des bibliothèques de requêtes pré-paramétrées et doit permettre de développer ses propres requêtes afin d'augmenter la base de cas d'usages en anomalie qui sont pistés ;

[TRA04] : le module d'analyse doit permettre une entrée par le patient, ou une entrée par le professionnel ;

[TRA05] : le module d'analyse des traces doit proposer un langage d'interrogation évolué et ensembliste de type SQL ;

[TRA06] : le module d'analyse des traces doit mettre en place des mécanismes de protection des logs (mise sous séquestre, séparation des tâches entre les administrateurs de la plateforme et les utilisateurs, etc.) de façon à rendre les traces juridiquement opposables ;

HABILITATIONS D'ACCÈS AUX DONNÉES MÉDICALES

Par le Docteur MAUDUIT, DIM du CHU de NANTES

Expérience et point de vue d'un médecin DIM

Le développement du dossier patient informatisé (DPI) questionne le cœur même de la pratique médicale. En effet, malgré la variété des spécialités et des types de prises en charge (programmées ou non, chirurgicales ou psychiatriques, transversales ou non), les protocoles de prescriptions, les transmissions infirmières ou encore la classification de la documentation ne peuvent plus être hétérogènes au sein d'un même établissement.

« Une certaine normalisation de l'utilisation du DPI est nécessaire pour assurer un partage efficace et sûr des données médicales. »

Une véritable transformation des pratiques est en cours et la confidentialité des données n'échappe pas à cette mutation.

L'accès au DPI peut se faire par plusieurs professionnels en même temps, où qu'ils soient physiquement et de métiers plus nombreux qu'auparavant, alors que le dossier papier ne pouvait être vu que par une personne à la fois et pas toujours dans son intégralité, certains services gardant un dossier patient « de spécialité ». L'accès au dossier papier étant restreint de fait, les professionnels redoutaient sans doute moins les accès illicites à celui-ci. Le DPI a par contre rendu le dossier patient parfaitement ubiquitaire et son déploiement a fait craindre une régression de la confidentialité des données du patient et des ruptures du secret médical plus fréquentes et facilitées. Lors du déploiement de son premier DPI, le CHU de Nantes a donc dû remettre certaines de ses pratiques en matière de confidentialité à plat.

Mais bien avant déjà, les droits d'accès aux données médicales de la Gestion Administrative des Malades (GAM), qui servait de DPI minimaliste de par la possibilité d'y conserver les courriers médicaux, avaient fait l'objet de révisions qui s'inscrivent dans une histoire commune à bien d'autres établissements. Il y a une dizaine d'années, les accès aux données médicales étaient limités en termes de type de personnels (essentiellement médecins et secrétaires médicales) et à la demande des patients un mécanisme (dit d'hyperconfidentialité) pouvait restreindre la visualisation aux seuls agents du service de prise en charge, non seulement des dossiers mais de l'existence même

des séjours. Cette limitation stricte ne pouvait se pérenniser. En effet, constatant des cas de perte de chance pour des patients (impossibilité de voir le dossier aux urgences par exemple) et parce que les médecins des services transversaux ou supports (unités mobiles diverses, radiologues, anesthésistes…) devaient pouvoir visualiser les dossiers de tous les patients, la liste des personnels autorisés à accéder aux « hyperconfidentiels » a dû s'élargir.
Cette constante recherche d'un équilibre entre le bénéfice d'un partage de l'information médicale et le risque d'une rupture de la confidentialité a encore été nécessaire récemment lors la première vague de la COVID-19. En effet, de nombreux agents ont dû être affectés en renfort dans des unités COVID, parfois du jour au lendemain. Les changements d'affectations dans les logiciels socles pour le calcul des droits d'accès ne pouvant matériellement pas être en permanence mis à jour, les droits ont dû être encore ouverts temporairement un peu plus largement.

Ces décisions ne tiennent (heureusement !) pas au seul médecin Dim, ni à la Direction des Services Informatiques, et l'Institution s'est dotée d'une instance en charge de la politique d'accès. Elle est composée de médecins, de la Direction Générale, de la Direction des Soins, de la Direction de la Qualité, du DIM et du Responsable de la Sécurité Informatique. Cette instance a donc défini une logique de contrôle a priori, la matrice des droits d'accès précisant pour chaque profession les modules accessibles (par exemple prescription ou non) et les actions possibles (écriture, utilisation de certains formulaires…).
En considérant que la nécessité de confidentialité débute avec la simple connaissance de la présence d'un patient dans telle ou telle unité, le nombre d'agent qui peut potentiellement accéder à de la donnée médicale est très élevé. Certes, accès possible ne veut pas dire droit d'accès et un agent doit toujours se poser la question de la légitimité de l'accès à un dossier médical, quelle que soit la possibilité technique qui lui en est donnée. Toutefois, l'expérience montre que le personnel n'est pas toujours au fait de ce qui est légal ou non, beaucoup (médecins compris) sont par exemple surpris que l'accès au dossier de leur propre enfant ne soit pas permis !

« Une ouverture plus importante des droits pour un meilleur partage des données doit donc aussi passer par une acculturation aux enjeux et droits en matière de confidentialité. »

Il faut former, informer, communiquer autant que possible, auprès de tous les agents sur ces sujets. Cela ne suffit bien sûr pas et c'est pourquoi le contrôle a priori doit absolument être accompagné d'une traçabilité des accès, c'est le contrôle a posteriori. Ce contrôle peut concerner des demandes particulières (un agent lui-même patient souvent) ou bien viser des patients ou groupes de patients, par exemple d'un service précis, qui ont demandé à être en hyperconfidentialité, ou encore VIP. Ces contrôles doivent découler d'un programme validé par l'Institution et les demandes et analyses sont l'objet d'un processus précis. Ils posent en revanche quelques problèmes qui rendent leur automatisation possible mais complexe.

Première limite, la volumétrie. Un seul séjour peut générer une quantité de traces inexploitables en détail et c'est un

travail de fourmi de rapprocher les agents tracés de leurs droits d'accès, ce jour-là, pour un patient donné. Autre problème : la granularité de l'analyse qui n'est pas toujours assez fine. Il est en effet parfois complexe d'extraire du DPI les accès par type de modules comme la visualisation de la prescription, des transmissions infirmières, des données d'identités ou encore des CRH. Les analyses sont plutôt réalisées en on/off : accès au dossier ou non.
Autre exemple de frein à l'automatisation complète de la détection des accès potentiellement illicites : les professionnels transversaux. Alors qu'on peut construire des alertes pour des cas d'accès aux dossiers de patients hospitalisés dans un service par des agents affectés à d'autres services, c'est quasiment impossible pour les professionnels transversaux car ils sont potentiellement en droit d'accéder à tous les séjours. Une coopération avec les services transversaux concernés est donc nécessaire pour auditer régulièrement les traces d'accès de leurs agents par confrontation avec d'autres données. On peut par exemple croiser les accès des Techniciens d'Etudes Cliniques avec des listes de patients inclus dans des protocoles. Du fait de toutes ces difficultés, l'instruction d'un potentiel accès illicite ne peut pas reposer sur une analyse uniquement « en chambre » mais doit être réalisée avec l'aide de la hiérarchie de l'agent éventuellement fautif, en lien avec les Ressources Humaines ou la Direction des Affaires Médicales. Et en cas de faute, ces directions doivent prononcer des sanctions. Les contrôles d'accès sont inefficaces s'ils ne sont pas suivis d'effets personnels et en matière de communication dans l'établissement.

Les accès évoqués jusqu'ici sont ceux du DPI et de la GAM mais il y a une multitude de logiciels dont les données médicales doivent aussi être protégées. Par exemple ceux relatifs aux rendez-vous ou les multiples logiciels de spécialités dont la politique de confidentialité se résume parfois à avoir différents profils génériques ! Ils ne doivent pas passer sous les radars de la politique de confidentialité de l'établissement. De même les entrepôts de données médicales doivent avoir leurs accès strictement encadrés ; il n'est pas question de déployer des outils d'interrogation des données médicales avec des accès qui seraient en contradiction avec la politique d'accès au DPI lui-même. Les possibilités d'interrogations des DPI eux-mêmes (de la base de production) sont en particulier à bien analyser sous cet angle.

Un Centre Hospitalier doit donc se doter d'une politique de confidentialité globale, dépassant le simple cadre du DPI, basée sur une analyse bénéfice / risque partagée et validée par des représentants médicaux et paramédicaux, développer un programme de traçabilité des accès efficace, former le personnel et communiquer sur les actions en lien avec la sécurisation des données médicales. Le prochain défi est celui de la mise en place d'un DPI et d'une GAM unique à l'échelle du Groupement Hospitalier de Territoire. Les établissements, dont les politiques en matière d'accès à l'information sont parfois bien différentes, ne pourront pas conserver leur mode de fonctionnement propre. D'une part le futur DPI ne proposera sans doute pas les mêmes fonctionnalités de contrôle d'accès que leur DPI actuel et d'autre part les attentes sont fortes en termes de partage de données entre établissements. Techniquement, pour pouvoir répondre à cet enjeu, le DPI

du GHT devrait pouvoir limiter les accès à certains profils, en écriture ou non, par sous-type de données (données administratives, CRH, formulaires, prescriptions…) plutôt qu'en on / off sur la quasi-intégralité du dossier patient. Cela pourrait permettre d'autoriser l'accès au dossier du patient tout en n'autorisant pas l'accès à de la donnée médicale. Par ailleurs les accès aux données médicales entre établissements différents doivent à mon avis être restreints aux médecins et quelques rares autres professionnels, quitte à paramétrer les droits individuellement. Concernant le contrôle des accès a posteriori, les différentes directions devront s'engager à la même politique de traçabilité et avoir la même conduite en cas d'accès illicite.

La difficulté sera donc de construire une politique de confidentialité commune au GHT, donnant assez de souplesse d'accès aux professionnels tout en garantissant la confidentialité des données. Avoir gagné en maturité sur cet enjeu dans nos établissements respectifs nous y aidera.

12. QUAND L'IA REMET EN QUESTION LES MODÈLES CLASSIQUES D'HABILITATION

Le Big Data et l'IA risquent de rebattre les cartes de la problématique des habilitations dans les années à venir.

En 2020, l'information selon laquelle un individu lambda a consulté en janvier pour la visite annuelle avec son ophtalmologue, en mars pour le dépistage du cancer colorectal et en juin s'est fait hospitaliser pour un problème de ménisque n'est à priori pas tellement sensible. Il s'agit de trois séjours ou consultations distinctes, sans réels enjeux de confidentialité (si le dépistage en question est négatif bien entendu).

Mais qui peut dire ce que le Big Data et l'IA pourront déduire, dans 15 ou 20 ans, de telles informations ? Peut-être que la conjonction de telles ou telles pathologies qui, prise isolément n'ont aucun impact, pourra donner une information capitale sur la santé présente ou les prédispositions du patient. Nul doute que l'information devient alors ultra-sensible et intéresse au plus haut point une bardée d'acteurs publics ou privés.

Il est donc probable que l'irruption de l'IA dans les prochaines années va rendre caduque certaines des conclusions ou suggestions du présent guide.

TRAÇABILITÉ, CONFIDENTIALITÉ, RESPECT DU SECRET MÉDICAL ET PROFESSIONNEL : ENJEUX ET OPPORTUNITÉS DU DOSSIER PATIENT INFORMATISÉ

Par Anne-Sophie MAURE DE LIMA, Directrice des Usagers, des Services aux Patients et des Partenariats Innovants du CHU de Nantes

Le point de vue d'un directeur d'hôpital

L'informatisation du dossier patient remet sur le devant de la scène le secret médical, comme son pendant, au cœur de toutes les règles de déontologie et d'obligations professionnelles, le secret professionnel. Ce dernier, défini par les articles 226-13 et 226-14 du code pénal, comme la discrétion professionnelle, définie par l'article 26 de la loi n° 83-634 du 13 juillet 1983 modifiée relative aux droits et obligations des fonctionnaires, s'imposent à tous. Quelles que soient ses fonctions, qu'elle soit fonctionnaire, salarié, agent public ou bénévole participant au service public, toute personne exerçant ou intervenant au sein d'un établissement de santé doit, aux patients accueillis, une confidentialité absolue sur l'ensemble des informations les concernant, que celles-ci soient personnelles, administratives, médicales et sociales[1]. Ce secret couvre ce que le professionnel a entendu, vu ou compris. Cela vaut aussi bien sûr pour ce qu'il a lu dans le dossier patient.

Au-delà du fait de ne pas révéler ce dont le professionnel a connaissance à l'occasion de son exercice professionnel, la loi prend une précaution supplémentaire: le professionnel de santé n'a le droit d'accéder qu'aux informations nécessaires pour la réalisation de ses missions. Ainsi, même si vous avez techniquement la possibilité d'accéder à tous les dossiers patients conservés par l'établissement, ce n'est pas pour autant que vous en avez le droit, en particulier pour ce qui concerne les informations médicales. En effet, celles-ci sont réputées confiées par le patient à l'ensemble de l'équipe de soins qui le prend en charge, dans la mesure où elles sont utiles à la continuité des soins ou si elles déterminent la meilleure prise en charge possible. Ainsi, l'accès aux informations contenues dans le dossier d'un patient n'est ouvert à un professionnel que pour préparer et assurer la prise en charge du patient concerné, et/ou en assurer la continuité. De ce fait, il faut avoir une bonne raison - professionnelle évidemment - pour accéder à ces données. Ces raisons ne peuvent être individuelles ; elles doivent être insti-

1 Article 9 de la Charte du patient hospitalisé - Loi du 04 mars 2002 relative aux droits des malades et à la qualité du système de santé, art. L1110-4 du Code de la santé publique.

tutionnellement définies.

L'informatisation ne change bien sûr pas ces principes fondamentaux mais elle en renforce les enjeux. La donnée n'a jamais été aussi facilement partageable, aussi consolidée et aussi regroupée qu'elle ne l'est aujourd'hui. En contrepartie, cette donnée, y compris toute action réalisée pour la consulter, la traiter, la supprimer, l'imprimer ou la communiquer, n'a jamais été aussi complète.
Désormais, aucun responsable hospitalier ne peut dire qu'il ne sait pas ce que font les personnes qu'il habilite au traitement de données : nous savons exactement qui fait quoi dans un dossier patient informatisé. Nous savons qui a accès à quoi, et par définition, pour faire quoi. Il n'a donc jamais été aussi facile de confirmer le respect des obligations professionnelles de nos équipes, même s'il ne faut pas oublier que la rupture de confidentialité n'est pas qu'informatique, elle peut être tout simplement humaine (parler d'un patient que l'on suit avec un collègue dans l'ascenseur bondé).
Dans le même temps, dans un monde où la transparence se développe et où tout est tracé, nous devons aussi veiller à la protection des professionnels, qui nous confient aussi leurs données et qui sont protégés dans ce cadre par le RGPD. Ainsi, comment faire cohabiter le droit du patient à décider à qui il confie les informations le concernant et la nécessité d'accès des professionnels pour faire leur travail ? Comment garantir le respect des règles d'accès au dossier patient ?

1. Habiliter

Le principe premier de la gestion des accès aux dossiers patients est une politique d'habilitation claire, définie collectivement et validée institutionnellement. Celle-ci peut-être plus ou moins restrictive, en fonction de la philosophie de l'établissement en la matière. Dans tous les cas, ces «droits d'entrée» doivent être écrits. Quelle que soit la philosophie définie, il y a aussi un enjeu que cette politique d'habilitation soit partagée par le plus grand nombre, en impliquant des professionnels de santé, de toute filière. De même, cette définition doit être partagée avec des représentants des usagers, à minima pour les informer, si ce n'est les consulter, sur la philosophie envisagée.
Une fois définie, cette politique d'habilitation doit être réévaluée régulièrement, au moins une fois par an, pour vérifier que les choix faits restent pertinents. De même, il faut veiller à ce qu'elle soit respectée strictement, notamment face aux demandes atypiques pour des professionnels dont l'exercice particulier ne rentre pas dans les cases génériques prédéfinies. Pour cela, des « gardiens du temple » doivent être identifiés pour instruire les demandes d'habilitations, notamment les plus spécifiques. Ils doivent être différents des professionnels qui habilitent concrètement les agents. De même, le caractère pluri professionnel de cette instance est essentiel (médecin, directeur des soins, juriste, informaticien, DPO, etc..). Enfin, un circuit de décision clair doit être posé, en cohérence

avec les organes de gestion, de pilotage et de contrôles des accès au dossier patient.

2. Sensibiliser

Le deuxième axe majeur est la nécessité de sensibiliser l'ensemble des utilisateurs du DPI à son fonctionnement, en particulier en ce qui concerne les règles d'accès et d'usages de cet outil de travail. La Haute Autorité de Santé demande d'ailleurs à chaque établissement de posséder un guide de gestion du dossier patient, largement diffusé, mais surtout connu de tous et appliqué au quotidien.
En matière d'habilitations, il s'agit d'abord de rappeler le droit, comme le sens des habilitations confiées au professionnel ; ces droits d'accès sont en effet confiés aux agents comme professionnel et non comme personne physique ou comme individu. Si le professionnel n'intervient pas dans la prise en charge d'un patient, même s'il s'agit de son enfant par exemple, il n'a juridiquement pas le droit d'accéder à son dossier patient directement, même s'il peut techniquement le faire.
En matière de sensibilisation, des outils de communication internes sont essentiels pour partager les bonnes pratiques de manière régulière, notamment au moment clef de l'arrivée du professionnel dans l'institution. Néanmoins, ces temps de sensibilisation et de formation doivent être incarnés, par des praticiens, des soignants, des directeurs, et être organisés régulièrement, en proximité, au plus près des professionnels. Cela vaut aussi bien sûr pour les stagiaires et internes, dont la formation initiale doit comporter un point dédié à ce sujet. Enfin, la formation continue doit aussi se saisir de cette thématique, en lien avec les droits des patients, l'éthique ou la déontologie.

3. Contrôler

De la même manière, que ce soit pour concrétiser ces actions de sensibilisation comme pour marquer les esprits, des contrôles réguliers doivent être opérés sur les accès des professionnels au DPI. Ils peuvent être programmés à l'avance sur un secteur identifié ou un profil métier, sur une sélection aléatoire d'accès, ou être réalisés à la demande d'un patient ou de l'encadrement d'un agent ou d'une équipe. Les situations des professionnels dont les accès sont complexes à contrôler (unités mobiles ou fonctions transversales par exemple) doivent être pensées spécifiquement car une simple analyse des traces n'est pas opérante. Ces contrôles sont majeurs, d'autant plus dans les cas où les habilitations sont larges et souples, puisque si le contrôle n'est pas fait a priori, il doit être fait a posteriori.
Plusieurs possibilités de contrôles sont envisageables, en fonction des

systèmes de traçabilité de chaque DPI. La philosophie peut être soit fondée sur une autorégulation des utilisateurs, dans les cas où le médecin référent du patient peut par exemple vérifier qui a accédé aux données du patient dont il est responsable. Elle peut aussi être beaucoup plus institutionnalisée, et reposer sur un système de contrôle centralisé, piloté par les responsables médicaux, soignants et administratifs du dossier patient. Cette deuxième voie me semble à préconiser, comme le pendant de la politique d'habilitation, en cohérence avec la responsabilité du chef d'établissement en la matière. Cela est d'autant plus important que l'une des problématiques majeures pour un hôpital est la situation d'un patient qui est aussi professionnel hospitalier. Le système de contrôle doit clarifier la façon dont cette situation est traitée, pour éviter la confusion des genres, et protéger l'encadrement de situations de tensions ou d'oppositions au sein d'une même équipe. Si la demande est faite comme patient, le professionnel doit être traité comme tel par la direction en charge des usagers par exemple, même si son accompagnement sur le plan professionnel doit être organisé par son encadrement ou la direction des ressources humaines ou des affaires médicales.

4. Sanctionner

La règle est claire, la sanction doit l'être aussi. En cas de résultats probants des contrôles réalisés, et une fois que le professionnel en cause a pu s'expliquer dans le respect des procédures disciplinaires existantes, les directions d'établissement doivent prendre la sanction qui s'impose, le cas échéant, dans le panel d'actions dont elles disposent. Les possibilités sont différentes entre le personnel médical et le personnel non médical. Pour autant, dans les deux cas, la direction se doit d'aller au maximum de ses possibilités d'actions, notamment en matière de signalement, car elle reste juridiquement responsable, notamment vis-à-vis du patient concerné.

La sanction doit bien sûr être proportionnée, notamment en ce qui concerne les conséquences sur les habilitations du professionnel concerné. En effet, on peut s'interroger sur les mesures à prendre en ce qui concerne les habilitations du professionnel en cause. Si la personne ne peut plus travailler, au risque de mettre en danger les patients, il n'est pas envisageable de couper ses accès sans y réfléchir à deux fois. Pour éviter ces situations, il est préférable de tirer les conséquences des accès indus repérés en ce qui concerne la politique d'habilitation de l'établissement, plutôt que les seuls accès individuels en cause. En effet, dans beaucoup de situations, cela permet de repérer des accès finalement peu pertinents ou encore une évolution nécessaire de la politique d'habilitation.

5. Signaler aux autorités compétentes

L'accès illégitime à un dossier médical, et encore plus l'usage inapproprié d'informations médicales, est pénalement répréhensible. Dans ce cadre, le directeur d'hôpital est fondé à signaler un délit potentiel au titre de l'article 40 du Code de Procédure Pénale au Procureur de la République.

Pour autant, le texte laisse une marge d'appréciation large. Il peut être pertinent de poser des critères à ce signalement, pour avoir la même grille de lecture et d'analyse des différentes situations, afin d'éviter des traitements différenciés, en particulier entre personnel médical et non médical. En matière de responsabilité pénale, le statut de la personne n'impacte pas cette obligation de signalement. On peut donc considérer que les situations dans lesquelles un préjudice est probable pour le patient, comme en cas d'accès indus réitérés, ce signalement se justifie clairement. On peut aussi considérer ce signalement comme systématique, même si cela en réduirait probablement la pertinence sur le long terme.

Au-delà du signalement au Procureur, d'autres signalements peuvent s'envisager, notamment pour le personnel médical. D'abord, pour les titulaires, un signalement au Centre National de Gestion peut se faire, comme autorité de nomination. Un signalement au Conseil de l'Ordre des Médecins est aussi possible. De manière plus large, un signalement aux ordres professionnels est envisageable pour toutes les professions qui en disposent.

6. Et le faire savoir

Ces différentes actions n'auront de réels effets, sur le long terme, que si elles sont connues des professionnels de l'établissement, non seulement pour participer aux actions de sensibilisation précédemment évoquées, comme pour rassurer sur le bon fonctionnement du système d'habilitation. Ainsi, les responsables du dossier patient veilleront à partager un reporting annuel sur les questions d'habilitations en instances, au-delà du seul Comité de pilotage responsable de la thématique.

Enfin, la question de l'information des patients concernés par des accès indus, au regard des obligations du RGPD en la matière, est importante. Un protocole doit être défini en la matière. Pour autant, il faut veiller dans ce cas à ne pas rompre soi-même son obligation de secret professionnel, ni à transmettre des informations sur les agents concernés, dont les données doivent aussi être protégées par l'établissement. Seule une réquisition peut lever cette protection, en cas de plainte déposée par la victime.

• • •

En conclusion, le directeur d'hôpital a une responsabilité importante dans l'application du droit et la prévention des risques associés à l'informatisation des dossiers patients et aux partages de données que la territorialisation, comme l'évolution des prises en charge dans une logique de parcours multi-entité juridique, imposent. Il a surtout une obligation de transparence vis-à-vis du patient qui a le droit d'accéder à son dossier médical, dans les conditions et les délais prévus par la loi, comme concernant la protection des informations le concernant ou le traitement de ses données.

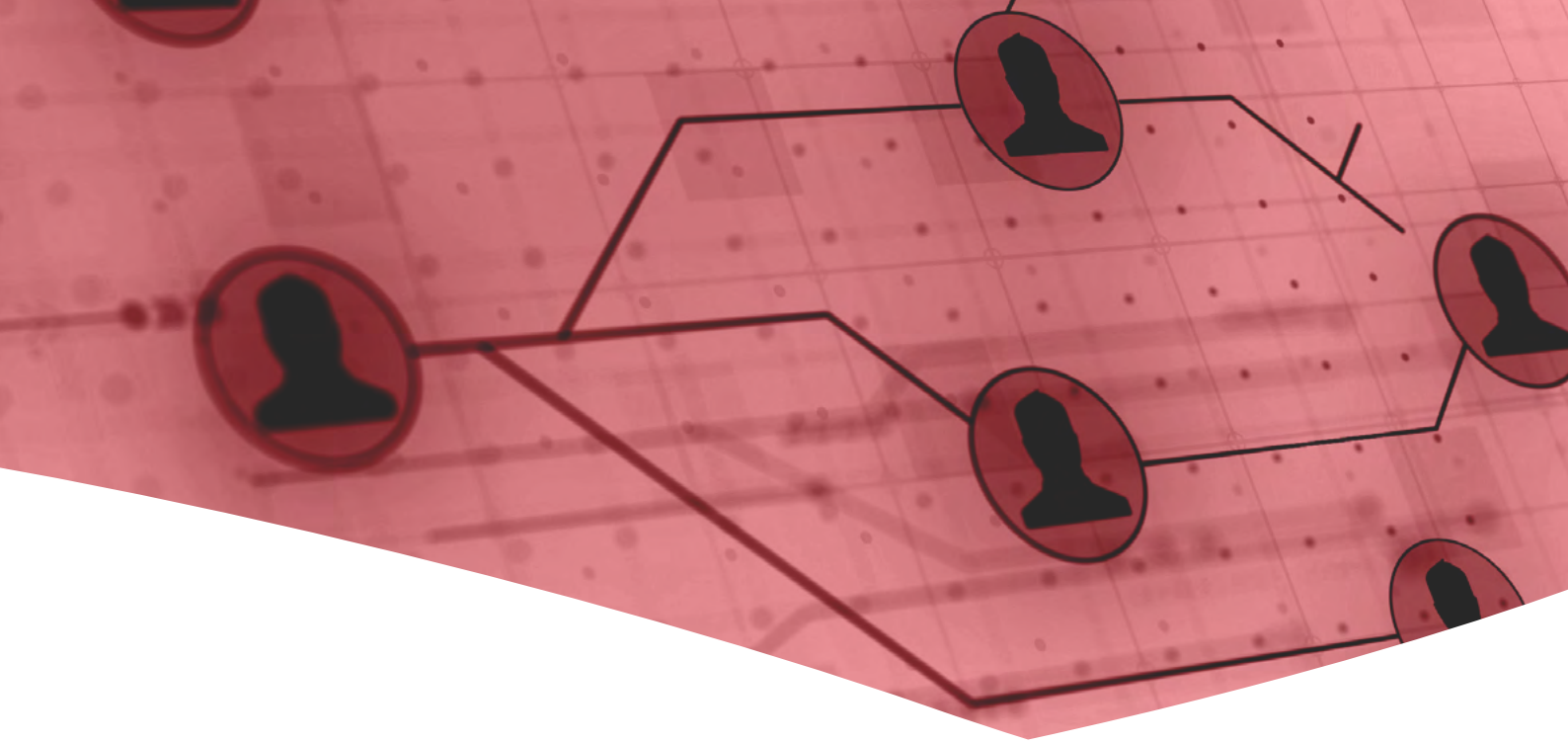
Sur ce sujet, comme sur d'autre, le sens du métier du directeur d'hôpital est de créer les conditions de soins de qualité, dans les meilleures conditions de sécurité possibles, pour le patient, comme pour les professionnels de l'établissement.

13. CONCLUSION

Pour soigner au XXIème siècle, il faut une prise en charge pluridisciplinaire, et donc partager de l'information. Ceci est totalement antinomique avec la notion de confidentialité : on peut tourner le sujet dans tous les sens pendant des heures, le partage augmente mécaniquement le risque de perte de confidentialité.

Et en même temps, la confidentialité n'est qu'un des trois piliers de la sécurité de la donnée, et cela n'est pas près de changer. La seule certitude est que le débat de la sécurité de la donnée médicale est éminemment collégial et que le pire risque est de s'enfermer dans une solution figée qui ne prenne pas en compte les changements sociétaux, qu'il s'agisse des évolutions réglementaires, des évolutions de la médecine à proprement parler ou des évolutions des technologies connexes telle l'IA.
C'est d'ailleurs bien dans l'esprit des normes et réglementations tel le RGPD ou l'ISO27001 que d'évaluer les risques, mais surtout de les réévaluer périodiquement.

Les modifications structurelles du système de santé (socle numérique national, GHT, etc.) sont en grande parties conditionnées par les questions d'habilitations d'accès, consubstantielles de la confiance et donc de l'efficacité et l'efficience des outils. Ces modifications se feront - ou ne se feront pas - selon que la question des habilitations aura été évaluée, débattue, tranchée.



APSSIS

Association Pour la Sécurité des SI de Santé

84 rue du Luart
72160 Duneau

06 29 36 59 95

secretaire@apssis.com

www.apssis.com

Création graphique : Corvy-Graphisme