Panorama de l'informatisation du secteur de la santé

Fabrice Mattatia (90),
responsable du Service relations clients, GIP CPS

Comme tous les secteurs professionnels, le secteur de la santé connaît depuis dix ans une évolution de ses pratiques liée à l'informatisation progressive des différents acteurs. La carte Vitale représente l'innovation la plus connue du grand public, mais le mouvement va bien au-delà du seul remboursement des soins aux assurés, et englobe aussi bien le suivi des dossiers des patients que les échanges entre professionnels libéraux ou hospitaliers, les envois de résultats d'analyses ou d'imagerie, la tenue des dossiers administratifs dans les établissements de soins, ou l'accès des professionnels à l'information sur les médicaments ou la recherche. Ces échanges, portant souvent sur des informations nominatives et confidentielles concernant les patients, et engageant la responsabilité de leur auteur (analyses, diagnostics), doivent bien sûr présenter toutes les garanties de sécurité sans lesquelles la confiance ne pourrait s'établir.

Les applications possibles de l'informatisation dans le monde de la santé

Les applications possibles de l'informatique sont nombreuses et touchent tous les domaines, au bénéfice tant des praticiens que des patients.

L'utilisation des moyens informatiques permet aux professionnels de santé de constituer et de mettre à jour les dossiers des patients (âge, antécédents, groupe sanguin, allergies, suivi médical, traitements passés ou en cours, et aussi radios, scanners, ou autres) sous une forme plus moderne et plus disponible que les traditionnelles fiches en carton. Cela rend également plus facile l'échange de ces informations, soit en les envoyant par *mail* à un confrère, soit en les rendant disponibles sur un serveur. Il est ainsi possible de stocker sur un serveur les informations de base concernant un patient ou son dossier d'hospitalisation, afin de permettre leur consultation par tout professionnel ayant à traiter ce patient, notamment en cas d'urgence.

Des réseaux de soins spécialisés peuvent également se constituer, reliant les différents professionnels (médecins, infirmiers, kinésithérapeutes et hôpitaux) ayant à collaborer dans le traitement de malades atteints de pathologies lourdes et chroniques.

Les nouvelles technologies permettent également aux praticiens d'échanger leur expérience et de demander des avis, en se communiquant rapidement des dossiers et des images, voire en pratiquant la télémédecine. Ils peuvent également accéder à des bases de données à jour sur les pathologies et les médicaments, et à des ouvrages médicaux et articles de référence.

Les gains de temps et d'efficacité ainsi acquis contribuent à améliorer la qualité de leur travail et des soins dispensés.

Enfin, la transmission d'informations complètes évite la répétition inutile d'actes comme les analyses ou

les différentes imageries, ce qui génère des économies. Les différents acteurs, aussi bien les établissements de soins que les assurances maladies obligatoires ou complémentaires, peuvent également améliorer la productivité de leurs services administratifs et médicaux. En analysant plus finement leur activité, ils peuvent en effet déceler des pratiques améliorables et des gisements de productivité.

En ce qui concerne la santé publique, les nouvelles technologies permettent une circulation plus rapide de l'information : en cas d'intoxication, d'épidémie, de mise en cause d'un produit ou d'un médicament, ou d'alerte à la suite d'un accident industriel, des renseignements précis peuvent être adressés par *mail* par les professionnels sur le terrain aux autorités sanitaires, lesquelles peuvent retransmettre par le même moyen à tous les professionnels concernés les consignes à suivre.

Les contraintes sécuritaires

La loi et la déontologie imposent des contraintes fortes lors de l'utilisation des nouvelles technologies dans le secteur de la santé.

Ces contraintes permettent de fonder la confiance que les acteurs peuvent s'accorder entre eux, et qu'ils peuvent accorder au système.

La première de ces contraintes, inscrite dans le Code de la santé publique depuis la loi du 4 mars 2002, est la confidentialité des données concernant les patients, aussi bien lors d'un échange ponctuel entre confrères, qu'à l'occasion de la mise sur serveur de dossiers ou de parties de dossier : les données doivent être protégées pour éviter toute lecture par des personnes non autorisées. S'il s'agit d'un *mail*, il faudra alors le crypter ; s'il s'agit d'un serveur de données, seuls les professionnels en charge du traitement du patient devront pouvoir accéder à ces informations, et, si le dossier est complet, ils doivent ne pouvoir accéder qu'aux seules informations dont ils ont besoin.

Ces restrictions nécessitent la mise en place d'une authentification *personnelle* de chaque intervenant.

Certains types d'informations doivent également être protégés de manière générale : il s'agit, par exemple, des publicités et informations sur les médicaments, qui légalement ne doivent pas être accessibles par le public. Les serveurs et les sites Internet pharmaceutiques doivent donc filtrer l'accès de leurs visiteurs, en s'assurant de leur qualité de professionnel de santé, mais sans avoir besoin de leur nom. Une authentification *professionnelle* est ici nécessaire.

La sécurité du patient exige que l'on puisse s'assurer de l'intégrité des données le concernant (penser à des résultats d'analyses ou à des prescriptions, pour lesquels toute modification intentionnelle ou non peut avoir des conséquences graves) et de la responsabilité de celui qui les a écrites. Ces garanties relèvent de la signature électronique, telle qu'elle a été reconnue par la loi du 13 mars 2000.

Dans le cas de données stockées sur un serveur, ou dans les systèmes informatiques des hôpitaux, il peut s'avérer utile de savoir qui a accédé à telle information et qui a modifié telle autre : cette traçabilité requiert la tenue d'un journal des accès et des modifications.

Il est également primordial, tant pour un dossier sur serveur que pour un envoi ponctuel, de s'assurer que les informations concernant le patient sont complètes et à jour. Aucune technologie ne pouvant assurer cela, il faut s'en remettre aux bonnes pratiques des intervenants.

Enfin il faut garantir l'accessibilité et la conservation des informations stockées sur serveur : un dossier perdu ou inaccessible ne sert à rien. Les responsables informatiques doivent veiller à la sauvegarde des disques, et à la redondance et au dimensionnement de leurs infrastructures, pour garantir la continuité et la pérennité de l'accès.

En résumé, les fonctionnalités indispensables pour fonder la confiance des professionnels de la santé dans les échanges informatiques sont principalement :
1) la confidentialité des informations,
2) l'authentification des personnes et des qualités,
3) l'intégrité des données,
4) la signature électronique des données,
5) la journalisation des accès et des modifications,
6) la sauvegarde régulière des données,
7) la redondance et le dimensionnement des infrastructures,
8) la définition de bonnes pratiques et leur respect.

Comment fonder la confiance ?

Dans la liste ci-dessus, la fonctionnalité n° 8 relève de l'organisation du travail. Les fonctionnalités 5, 6 et 7 sont du domaine de l'administration et de l'exploitation informatiques classiques. En revanche les quatre premières fonctionnalités ne sont pas encore répandues dans l'utilisation des nouvelles technologies.

Pourtant, ces quatre fonctionnalités ne constituent en rien une nouveauté : elles sont indispensables à la confiance depuis que l'écriture existe et que l'on communique des informations sensibles. Il y a six mille ans, les Mésopotamiens utilisaient déjà des sceaux-cylindres pour " sécuriser " leurs messages rédigés sur des tablettes d'argile : l'expéditeur disposait d'un sceau orné personnel, servant à l'authentifier. En roulant son sceau en surimpression sur le message, il le signait. Il pouvait enfin placer la tablette dans une " enveloppe " faite d'une boule creuse d'argile, et apposer encore une fois le sceau sur la boule : l'intégrité et la confidentialité du message étaient ainsi garanties pendant le transport.

Le Louvre possède ainsi le sceau d'un médecin sumérien qui exerçait à Ur en 2100 avant notre ère, preuve que le secteur de la santé se préoccupait déjà, à l'époque, des problèmes de confiance !

Toutefois, ce système de sceaux, qui perdura en Europe sous différentes variantes jusqu'au XIX[e] siècle, ne permettait d'accorder sa confiance qu'à des interlocuteurs connus, dont on reconnaissait le sceau. Aujourd'hui, l'informatisation des échanges implique de devoir accorder sa confiance à des interlocuteurs parfois inconnus : le professionnel doit alors pouvoir véri-

© PHOTO RMN.

Le sceau du médecin Ur-Legal-Edina, 2100 av. J.-C., Lagash. Louvre, albâtre.

fier leur identité et leur qualité avant de les croire ou de leur accorder des droits d'accès à un système d'informations.

Il faut donc trouver un moyen de garantir cette identité et cette qualité lors d'échanges électroniques. Pour cela, la technique et l'organisation constituent les deux piliers sur lesquels fonder la confiance et la sécurité.

Techniquement, des solutions existent. Le secteur français de la santé s'est doté d'une infrastructure de gestion de clés (IGC) répondant aux normes en vigueur, afin de permettre à chaque professionnel de disposer de certificats électroniques garantissant son identité et sa qualité [1]. Plus de 430 000 personnes sont en possession aujourd'hui d'une carte à puce, dite Carte de professionnel de santé (CPS).

La carte CPS contient les certificats et les clés nécessaires à son porteur pour :

- garantir son identité et sa qualité,
- signer électroniquement (au sens de la loi sur la signature électronique) ses *mails* ou ses documents et en garantir l'intégrité,
- chiffrer des informations pour les rendre confidentielles,
- s'authentifier pour accéder, de manière confidentielle, à des systèmes d'informations ou à des serveurs *Web* réservés.

Cette IGC est conforme aux standards depuis novembre 2001 (certificats X509v3 – nous n'insisterons pas sur ces notions techniques) et son utilisation est possible avec tous les matériels, logiciels et fournisseurs d'accès Internet, permettant ainsi l'universalité et l'interopérabilité des solutions de sécurisation.

La CPS constitue donc à la fois une "carte d'identité électronique" et un "sceau électronique", mais cela ne présume en rien de l'usage qui en sera fait. Il revient aux applications mettant en œuvre ses fonctionnalités de s'en servir à bon escient.

La balle est désormais dans le camp des développeurs d'applications et des éditeurs de logiciels : à eux d'intégrer systématiquement l'usage de la CPS dans les applications et systèmes d'informations du secteur de la santé, pour gérer le filtrage des accès, la gestion des droits des intervenants, la traçabilité des actions, etc.

Toutefois, la technique n'est rien sans l'organisation : avant de distribuer des certificats, il a fallu concevoir les circuits et les procédures administratives permettant de collecter et de garantir les informations à certifier. La collaboration indispensable des ordres professionnels, de l'État, des caisses d'assurance maladie obligatoires et complémentaires, et des représentants des utilisateurs, s'est concrétisée dans la création en 1993 d'un groupement d'intérêt public (GIP), le GIP CPS, chargé de mettre en œuvre les solutions nécessaires à la confiance dans les échanges électroniques du secteur. Outre l'IGC citée ci-dessus, le GIP CPS a élaboré les procédures, regroupant toutes les autorités du secteur, et garantissant la fiabilité des informations utiles : identité, diplôme, spécialité, activités, lieux d'exercice…

Les aspects organisationnels sont également présents lors de l'utilisation quotidienne des applications techniquement sécurisées : il est au minimum indispensable que ces applications s'intègrent sans heurt dans l'organisation du travail des professionnels, dans les cabinets ou les établissements de soins. Si l'ergonomie se révèle inadaptée, ou les contrôles sécuritaires fastidieux, les utilisateurs rejetteront l'application.

Même lorsque l'application sait rendre service en faisant oublier les contraintes, les professionnels doivent de leur côté veiller à une stricte discipline dans l'application des règles de sécurité : protection des codes secrets et des cartes à puce, bonne définition des droits d'accès aux informations stockées dans les bases ou les disques durs, etc. Or le secteur de la santé, dans lequel l'informatisation est récente, ne possède pas encore une réelle culture de sécurité informatique.

Les applications concrètes

Nous avons évoqué plus haut des usages potentiels. Quels sont ceux déjà concrétisés ?

62 % des professionnels attendent de la CPS qu'elle participe à la sécurisation de leur poste de travail, et 52 % qu'elle serve à protéger les documents sensibles. Pour 65 % des médecins généralistes utilisant l'informatique, elle est indispensable pour sécuriser les *mails* échangés dans le cadre de leur activité [2].

Des messageries sécurisées utilisant la CPS sont désormais sur le marché : elles permettent la signature et le chiffrement des messages. Il est ainsi possible d'envoyer des informations à un confrère de manière sécurisée.

Plusieurs établissements, comme les hôpitaux universitaires de Strasbourg (HUS), utilisent la CPS pour permettre à leur personnel d'accéder au système d'informations profitant du fait que la carte à puce avec code secret est un moyen plus sûr que le simple mot de passe traditionnel, qui peut être espionné ou prêté.

D'autres, comme le Centre hospitalier de l'arrondissement de Montreuil-sur-Mer (CHAM), ont mis les dossiers médicaux de leurs patients sur serveur, afin que les patients et leurs médecins traitants y aient accès [3].

Il est envisageable de pousser encore plus loin cette logique de relation *via* Internet entre l'hôpital et l'extérieur. Ainsi, aux États-Unis, le *Beth Israel Deaconess Medical Center* de Harvard propose à ses patients un site Internet sur lequel ils peuvent dialoguer avec leur médecin, lui demander une prescription (qui sera directement envoyée à la pharmacie de leur choix), prendre un rendez-vous, consulter la facturation des actes effectués dans l'établissement ou leur dossier médical et l'historique des prescriptions effec-

tuées, consulter les archives de leurs résultats d'analyses, d'électrocardiogrammes, de radios, etc.[4]

En France, plusieurs réseaux de soins spécialisés, centrés par exemple sur une pathologie ou sur le suivi de patients, utilisent Internet pour échanger des informations. Par exemple, le réseau Ammelico regroupe 95 % des laboratoires d'analyses médicales et plusieurs centres hospitaliers du Nord-Pas-de-Calais, et transmet 50 000 pages de résultats par mois[5].

D'autres réseaux relient les différents professionnels collaborant à la prise en charge de patients atteints de pathologies lourdes : médecins, analystes, infirmières, masseurs-kinésithérapeutes, etc., et permettent la circulation rapide des informations. Circulation rapide qui est également l'objectif des réseaux centrés sur les attentes de greffes, pour lesquels une réaction en temps réel est primordiale.

Autre application : pour diffuser les alertes sanitaires, le ministère de la Santé met en place une base de données des adresses électroniques des professionnels volontaires. Un simple clic permettra ainsi de les avertir tous simultanément en cas de crise[6].

Le dossier médical en ligne : une expérience québécoise

Un des projets actuellement envisagés en France est la création pour chaque patient d'un dossier médical centralisé disponible sur serveur.

Cette idée suscite de nombreux débats, tant auprès des patients inquiets pour l'accessibilité et la confidentialité des données, que chez les professionnels.

Il peut être utile de noter que ce type d'application est également étudié au Québec et y a déjà donné lieu à une expérimentation, dans le cadre du projet PRSA Carte Santé. Ce projet consistait à stocker des renseignements cliniques (allergies, diagnostics, vaccination, traitements, résultats d'analyses, suivi médical) dans un dossier médical centralisé (dit "Dossier carte santé" ou DCS), localisé au siège de l'assurance maladie, en gérant le consentement du patient pour chaque inscription d'information et chaque consultation.

Quelques chiffres

L'application la plus répandue est le système Sesam-Vitale, qui permet aux assurés, porteurs d'une carte à puce Vitale décrivant leurs droits, de bénéficier d'un remboursement plus rapide.

57 millions de cartes Vitale étaient en circulation en octobre 2002.

Les professionnels de santé utilisent quant à eux leur carte de professionnel de santé (CPS), qui certifie leur identité et leur qualité, et leur permet de signer les feuilles de soins électroniques (FSE) du système Sesam.

135 000 professionnels de santé (soit 60 % des médecins et 73 % des pharmaciens) collaboraient à Sesam en septembre 2002, en créant plus de 49 millions de FSE par mois, ce qui correspond à la dématérialisation de la moitié environ des feuilles de soins[7].

Il a été émis plus de 430 000 cartes de la famille CPS, dont 230 000 cartes pour les professionnels libéraux et hospitaliers, et plus de 200 000 pour les employés. 80 % des médecins libéraux et plus de 90 % des pharmaciens sont équipés.

Les établissements de soins ne sont encore que marginalement équipés[8].

Un rapport de l'expérimentation a été rédigé[9]. Les patients, favorables au partage d'informations entre les professionnels qui les traitent, ont apprécié ce principe. En revanche les professionnels, pourtant intéressés par l'accès aux dossiers d'autres établissements, ont majoritairement été déçus.

Parmi les principaux reproches exprimés par les professionnels figurait le fait que le DCS n'est qu'un résumé de dossier, toutes les informations se trouvant dans le dossier médical du praticien. Du coup, remplir le DCS représente un fardeau inutile ; les professionnels ne le remplissent pas, ne le consultent pas et lui préfèrent le dossier complet. Par ailleurs l'obligation d'obtenir le consentement du patient avant tout remplissage du DCS inquiète les professionnels car elle remet en question la complétude des données. Ils ne font pas confiance à un dossier potentiellement incomplet.

Pour remédier à ces inconvénients, le rapport suggère d'étudier le concept d'un dossier médical virtuel, composé d'accès à plusieurs bases de données sécurisées, ou à plusieurs dossiers partiels éparpillés (dans les laboratoires, les hôpitaux, les cabinets, etc.), contenant chacun une partie des informations sur le même patient. La carte du patient servirait dans ce cas à contenir les pointeurs et les clés d'accès vers ces bases.

Conclusion

L'informatisation du secteur de la santé ouvre des perspectives innombrables pour l'amélioration de la circulation de l'information et des connaissances, participant ainsi à l'amélioration de la qualité des soins. Cette évolution bénéficiera aux professionnels de santé et aux patients.

La sécurité représente une contrainte forte dans ce secteur. Les outils techniques permettant de fonder la confiance sont désormais opérationnels et disponibles. Il revient maintenant aux professionnels de se les approprier, et aux éditeurs de logiciels de les intégrer dans toutes les applications qu'ils pourront inventer. n

---

1 - Voir mon article dans *La Jaune et la Rouge* de décembre 1999.

2 - Sondages réalisés en décembre 2000 auprès de 535 médecins généralistes utilisant l'informatique et de 1 343 professionnels de santé. Détails sur www.gip-cps.fr

3 - www.ch-montreuil.fr

4 - www.bidmc.harvard.edu, rubrique Our services/Patientsite

5 - www.quotimed.com – article du 24 octobre 2002.

6 - Arrêté du 30 septembre 2002.

7 - www.sesam-vitale.fr

8 - Chiffres de novembre 2002. Pour plus d'information, voir www.gip-cps.fr

9 - www.ramq.gouv.qc.ca – rapport également disponible sur www.gip-cps.fr