

Des données santé pas si anonymes que ça

Des milliers de données santé sont accessibles aux chercheurs via la plateforme eHealth. Pour certains, l'anonymat des patients ne serait pas suffisamment protégé.

• **Caroline DESORBAY**

On a beaucoup débattu de la protection des données santé dans le cadre du dossier médical partagé pour lequel le patient doit donner son accord. On a beaucoup moins évoqué la confidentialité des données médicales collectées pour alimenter des registres relatifs à certaines pathologies, épidémies ou à la santé publique. L'accès à ces infos santé, parfois très détaillées, se fait via la plateforme d'échange eHealth, sans l'aval des patients.

Des registres très utiles mais parfois inutilement nominatifs

Personne ne conteste l'importance de ces bases de données qui améliorent les soins de santé en facilitant le travail des chercheurs. Elles évitent aux médecins traitants et aux hôpitaux de devoir encoder plusieurs fois les mêmes données santé. Patients, personnel soignant, gestionnaires de la santé... tout le monde devrait s'y retrouver.

Là où ça coïncide pour certains, c'est dans le traitement des données qui ne garantirait pas suffisamment l'anonymat des patients.

David Simon, médecin généraliste, a été pendant plusieurs

années conseiller technique au conseil national de l'Ordre des médecins. Il s'inquiète du fait que les nom, prénom et lieu de résidence figurent dans ces registres. « Il y a quelques jours j'ai eu accès via le site Healthdata.be à des données collectées dans un registre appelé IPQED. On y trouvait toutes les données de santé concernant des patients diabétiques : type de diabète, historique des traitements médicaux et chirurgicaux, habitudes tabagiques, poids, taille, tension artérielle, hypoglycémies... C'est tellement précis et daté que l'on peut pratiquement reconstituer le dossier médical complet de chaque patient. Le plus interpellant, c'est que le nom, le prénom, la date de naissance, le sexe et le lieu de résidence du patient y sont également inscrits ».

Se protéger d'éventuelles dérives

Pour ce médecin, le fait qu'eHealth attribue un numéro aléatoire et crypté en lieu et place des nom et prénom du patient ne suffit pas à garantir définitivement l'anonymat des patients. « À partir du moment où il existe un lien fut-il conservé par un tiers de confiance comme eHealth, il reste techniquement possible d'identifier la personne au départ de ce code. On peut très bien imaginer par exemple qu'un futur

gouvernement ultralibéral autorise la "réidentification" des patients afin de traiter ces données dans une finalité autre que celle qui a guidé leur récolte auprès des médecins, pour le plus grand bonheur par exemple de l'industrie pharmaceutique, des compagnies d'assurances ou des employeurs. »

Pour le Dr Simon, « seules les données agrégées peuvent prétendre être "anonymisées" : lors de leur collecte auprès des médecins, on les sépare irréversiblement de tout code qui permettrait de retrouver l'identité du patient et le fichier de données personnelles demeurerait bien en sécurité chez les médecins qui ont exporté des données réellement anonymisées ».

« Manque d'indépendance »

Le médecin généraliste regrette aussi qu'eHealth soit le tiers de confiance chargé de conserver la table de conversion entre le pseudo-crypté et l'identité de la personne. « En effet, eHealth manque d'indépendance par rapport au pouvoir politique exécutif. »

L'inquiétude des médecins a été relayée au Parlement. Le 23 février dernier, la députée cdH Catherine Fonck a interpellé Maggie De Block à ce sujet. « Tant que ces données médicales sont uniquement consultées par

le personnel soignant, il n'y a pas de problème mais les verrous censés en interdire l'accès à d'autres personnes sont pour moi loin d'être suffisants », s'inquiète Catherine

Fonck. « La ministre De Block prône le Big Data pour faciliter la recherche mais on est en droit de s'interroger sur le devenir des données médicales une fois les recherches terminées ». ■

« C'est tellement précis et daté que l'on peut reconstituer le dossier médical de chaque patient. »

Une vingtaine de registres

En novembre 2015, l'Inami et l'Institut scientifique de Santé publique (ISP) ont conclu un accord sur la standardisation de l'enregistrement de certaines données de santé par le biais

de la plateforme Healthdata.be. « Très schématiquement, Healthdata.be permet de transférer une donnée codée du point A au point B, de manière fiable et totalement sécurisée grâce à un système de double cryptage », précise Johan Van Bussel de l'ISP. Le KCE et l'ISP ont répertorié plus de 150 bases de données relatives à la santé,

disponibles sur Healthstat.be. En 2016, une vingtaine de registres sont ouverts sur Healthdata.be, concernant notamment des maladies (diabète, mucoviscidose, sida...), la surveillance de maladies liées au milieu hospitalier... Une douzaine d'autres registres sont annoncées pour 2017.

INTERVIEW • Frank ROBZEN

« Tout est mis en œuvre pour sécuriser l'échange des données de santé »

Frank Robben vous êtes l'administrateur général de la plateforme eHealth et membre de la Commission de protection de la vie privée. Doit-on être inquiet concernant l'anonymat de nos données de santé ?

Non car tout a été mis en œuvre pour que l'échange d'informations via la plateforme eHealth soit bien protégé et bien sécurisé. Les données collectées ne peuvent être communiquées qu'à des chercheurs et à des médecins ayant obtenu l'autorisation du Comité sectoriel de la sécurité sociale et de la santé qui dépend de la Commission vie privée. Les recherches en question doivent impérativement œuvrer à l'amélioration des connaissances, de la qualité et de la gestion des secteurs de la santé et des soins de santé.

Le fait que la plateforme eHealth se charge des échanges et soit aussi le tiers de confiance inquiète certains médecins...

Je peux comprendre qu'il y ait des craintes parce que eHealth est un organisme de l'État et certaines informations proviennent aussi de l'État. Mais on est une plateforme d'échange, on ne

détient pas les données de fond qui restent chez les médecins, dans les hôpitaux... bien à l'abri dans des logiciels sécurisés. Le tiers de confiance doit être indépendant vis-à-vis de celui qui détient les informations et vis-à-vis de celui qui reçoit les données pour la recherche. Nous, on ne fait aucune recherche, on n'est pas géré par des chercheurs mais par des instances censées défendre soit l'intérêt des patients, soit l'intérêt des prestataires de soins. Il ne faut pas avoir peur de son ombre.

Et puis, eHealth est une petite institution parastatale qui dépend d'un comité de gestion au sein duquel les prestataires de soins, les mutualistes et les institutions publiques sont représentées à parts égales. Ce qui revient à dire que ce sont les personnes chez qui on prélève les données santé qui sont nos patrons.

Enfin, aucune transmission de données n'est possible sans l'aval du Comité sectoriel validé par le Parlement. J'ai toujours fait en sorte qu'il y ait un contrôle indépendant sur le fonctionnement de la plateforme eHealth.

Quelle est votre position par rapport aux éventuelles dérives du système qui pourrait servir les intérêts de l'industrie pharmaceutique, des employeurs, des compagnies d'assurances ?

Les registres ne sont pas faits pour contrôler les gens mais pour mieux les soigner et faciliter les études scientifiques. Je n'ai jamais eu la moindre demande concernant la plateforme eHealth allant dans le sens d'un contrôle. Quant à l'industrie pharmaceutique, si elle a parfois besoin d'un feedback après avoir testé des médicaments en milieu hospitalier, cela se passe dans un cadre légal fixé bien avant le lancement de la plateforme eHealth.

Depuis 25 ans, la banque Carrefour de la sécurité sociale (NDLR : Frank Robben en est aussi l'administrateur général) centralise des données sociales... L'Inami et les mutualités n'ont pas accès aux données concernant les chômeurs excepté quand ils en ont besoin pour introduire les allocations sociales. Je ne vois pas pourquoi il en irait autrement pour eHealth. ■ **Ca.D.**

DÉCODAGE

Un malaise compréhensible

Jean-Marc Van Gyseghem est avocat, spécialisé dans les données à caractère personnel relatives à la santé. Il est également membre du CRIDS, Centre de recherche information droit et société basé à Namur. Il nous apporte son éclairage sur la question des données échangées via la plateforme eHealth.

1. Malaise Les données de santé sont considérées comme des données sensibles et doivent être à ce titre extrêmement bien protégées, rappelle l'avocat. « Je ne suis pas en mesure de dire si la plateforme eHealth protège bien ou mal les données des patients, cela dépend du type d'algorithme mis en place. Mais je peux comprendre le malaise des médecins dû au manque de transparence. Ils sont détenteurs du secret médical qu'ils sont légalement tenus de protéger à juste titre et on leur demande de fournir des informations relatives à leurs patients sans avoir la garantie que ces

données sont anonymes. Quand un traitement n'est pas transparent, il pose question même s'il est légitime. La transparence est un des principes centraux de la loi de 1992 sur la protection des données personnelles ».

2. Codeur externe

L'avocat évoque l'arrêt royal de 2001 « qui précise que c'est plutôt la personne qui transmet les données qui doit les coder. Si ce sont des données qui proviennent de diverses parties et vont vers un seul récipient, il faut à ce moment-là un codage effectué par une personne tierce que l'on appelle organisme intermédiaire ». La plateforme eHealth exerce cette fonction en toute légalité mais le fait que les données santé des patients « tournent en vase clos » inquiète le corps médical. « Il suffirait de peu de chose pour rassurer les médecins en confiant la table de conversion à un codeur externe tout à fait indépendant de la plateforme eHealth. On éviterait ainsi la

confusion des genres ».

3. Nécessité Pour l'avocat, le fait que le patient ne soit pas averti que ses données santé sont utilisées ni à quelle fin pose problème. « L'article 8 de la Convention européenne des droits de l'homme précise que l'ingérence dans la vie privée doit être nécessaire. Cette nécessité existe à deux niveaux : le traitement des données doit être le moins invasif dans la vie privée – si on peut utiliser des données anonymes pour une recherche, il faut le faire – et la collecte des données doit se limiter aux informations nécessaires. Ici, on collecte un maximum de données pour des recherches potentielles or c'est une recherche bien précise qui devrait déterminer les données à récolter. » ■ **Ca.D.**

« Il serait rassurant pour les médecins de passer par un codeur indépendant de la plateforme eHealth. »