Le partage de données numériques de santé

lundi 21 juin 2021

Les données numériques de santé devraient-elles être partagées avec l'industrie et/ou la recherche? Oui, mais…!

Un article paru il y a peu dans le Tagesanzeiger suscite de nombreuses réactions. Devrions-nous partager les données de santé de notre futur dossier électronique avec la recherche privée ou universitaire? Il y a de bonnes raisons de le faire, comme il y en a de s'y refuser. Le conseil consultatif numérique de la Société suisse SEP propose une analyse de la situation.

Les données numériques – le nouvel or noir?

De nombreuses entreprises doivent leurs revenus à la production quotidienne de données personnelles. Toutes les personnes disposant d'un appareil équipé d'une connexion à Internet laissent derrière elles des traces numériques. Même les logiciels que l'on peut utiliser gratuitement ont un prix. Ils se payent avec des données personnelles. Les données numériques ont des spécificités attrayantes. On peut les copier, les envoyer rapidement par voie électronique, les modifier et les réunir aisément, les associer sans effort et les enregistrer de manière compacte. L'analyse de données, même en grandes quantités, est rapide à réaliser. Par rapport au bon vieux courrier postal, il est évident que le traitement des données sur papier (contrairement aux e-mails) était bien plus fastidieux.

Pourquoi les données numériques sont-elles si précieuses?

Les spécificités évoquées plus haut sont l'une des raisons qui font que ces données sont si précieuses. Le fait de pouvoir réunir et mettre en relation ces résidus de données permet d'obtenir une image assez précise de la personnalité ou des habitudes d'un individu. Vous trouvez cela invraisemblable? Et pourtant c'est exactement ce qui se passe sur Internet lorsque vous voyez des bannières publicitaires. De nombreuses grandes entreprises du Web font recette en proposant de la publicité aussi adaptée que possible, c'est-à-dire des annonces ciblées, à même de capter notre attention le plus longtemps possible.

Les données numériques confèrent également un certain pouvoir. Imaginez qu'une boutique en ligne ait connaissance de vos revenus et qu'elle adapte ses prix en fonction (plus vous gagnez, plus ils sont élevés). On sait déjà que ces boutiques affichent des prix différents en fonction de la région grâce à l'adresse IP (qui donne des informations sur la zone de résidence). Pour de nombreuses entreprises, il est aujourd'hui tout à fait normal de consulter les publications sur les réseaux sociaux,

que ce soit celles des personnes qui postulent pour un emploi chez elle ou celles d'un organisme avec qui elles souhaitent entamer une collaboration.

Dans le domaine de la santé aussi, les données sont précieuses. Les médicaments ainsi que les traitements sont longs à mettre au point et ont parfois dû être testés sur des milliers de personnes. Ceci coûte énormément d'argent et la collecte de données de santé permet de réduire la durée de telles études (ou au moins d'en accroître l'efficacité). Et au fond, c'est une bonne chose. Tout le monde profite de manière plus ou moins directe du progrès médical. Le partage de données n'est pas une mauvaise chose en soi. Tout dépend des conditions encadrant le contrôle et la protection de la vie privée.

Protection des données et conditions d'utilisation obscures

En Suisse, la protection des données est considérée comme assez stricte. La Constitution stipule que: «Toute personne a droit au respect de sa vie privée et [...] a le droit d'être protégée contre l'emploi abusif des données qui la concernent.» Le Règlement général sur la protection des données (RGPD) de l'UE, duquel la nouvelle loi suisse en la matière s'inspire, a renforcé une fois de plus la protection des données par le biais d'une réglementation plus ferme, mais également très complexe. Mais la loi laisse toutefois un peu de marge de manœuvre. Et certains aspects ne sont pas suffisamment encadrés.

En outre, le comportement personnel des utilisateurs aplanit volontairement de nombreux obstacles et oscille entre consentement résigné (ils savent déjà tout sur moi de toute façon) et incertitudes pénibles (mes données sont-elles 100% en sécurité?). Seul un très petit nombre d'individus prend le temps de bien lire les conditions générales de vente ou d'utilisation d'un logiciel ou d'une application. Pour rendre tout cela encore plus compliqué, les conditions générales sont souvent écrites en tout petit et dans un jargon juridique complexe, elles véhiculent donc un sentiment d'incertitude. Transfert des données vers l'étranger? Sauvegarde des données dans un cloud (c.-à-d. sur plusieurs serveurs en même temps)? Mise en relation des données avec votre profil sur les réseaux sociaux? Utilisation des données de géolocalisation de votre smartphone pour un meilleur service? En cliquant sur «Accepter», on offre souvent carte blanche aux entreprises. Dès lors que l'on n'est pas d'accord avec tout cela, la seule alternative reste bien souvent de ne plus avoir le droit d'utiliser le logiciel, l'application ou le site dont on a précisément besoin.

Tout ceci est légal, mais pas vraiment favorable à l'utilisateur. Dans ces exemples, il ne s'agit pas d'un problème de protection légale des données, mais plutôt de manque de transparence et de manque de confiance. Que faire?

Quelques règles générales pour s'y retrouver dans jungle de la protection des données

Il n'existe malheureusement pas de règles universelles, mais il peut être judicieux de garder à l'esprit quelques principes (sans prétendre à l'exhaustivité).

Toutes les données sont précieuses!
Dès lors qu'elles sont disponibles en grandes quantités et/ou mises en relation avec des informations complémentaires, même les données qui semblent sans valeur sont substantielles. Leurs champs d'application dépassent souvent notre imagination. Aucune donnée n'est dépourvue de valeur. Aussi, essayez de savoir dans quel but les données sont collectées ou traitées.

Si c'est gratuit, c'est vous le produit.
Voir le point 1!

Traitement des données à des fins commerciales ou de recherche?
La recherche non commerciale est encadrée plus strictement que de nombreuses analyses à des fins commerciales, du moins en Suisse. La recherche est définie comme «une quête méthodologique de connaissances généralisables». Lorsqu'un projet de recherche porte sur des données de santé, celui-ci doit généralement être validé par une commission d'éthique cantonale. Ce n'est certes pas un gage absolu de qualité et de protection des données, mais cela reste une vérification supplémentaire des intentions. Plusieurs critères entrent en jeu en fonction du degré d'anonymisation. Les projets commerciaux (p. ex. l'analyse de banques de données existantes au sein d'une entreprise) peuvent parfois déroger à cet examen. Aussi, regardez s'il y a eu une validation par une commission d'éthique ou au moins un examen par un responsable cantonal de la protection des données.

Mes données m'appartiennent-elles vraiment?
Vérifiez si vous pouvez retirer votre consentement au traitement des données et essayez d'en connaître la procédure. Les données seront-elles ensuite supprimées ou entièrement anonymisées (cette dernière option est le processus prescrit par la loi pour ce qui est de la recherche)? Cela s'applique-t-il aussi aux données dans le cloud et dans les backups? Qu'adviendrait-il de mes données si la société faisait faillite? Combien de temps les données sont-elles conservées?

Les données sont-elles associées au niveau individuel à d'autres banques de données?
Si oui, quelles données, et d'où proviennent-elles? Pouvez-vous refuser l'association des données? Cette mise en relation est-elle temporaire (relative à un projet) ou définitive? Les données associées peuvent-elles être transmises à des tiers?

Avez-vous un droit de regard ou de participation?
Pouvez-vous refuser le traitement ou le partage de certaines données que possède déjà l'entreprise/l'unité de recherche?

Les données sont-elles susceptibles de passer une frontière nationale?
Si tel est le cas, il y a un risque de perte de contrôle. À chaque pays son droit natio-

nal. Vous donneriez-vous la peine de faire valoir vos droits dans un autre pays qui dispose d'un système juridique étranger?

Pouvez-vous trouver des informations accessibles publiquement qui répondent à toutes ces questions?
Vous pourrez certainement trouver des informations concernant certains des points évoqués, mais probablement pas tous. Et il n'est pas impérativement nécessaire d'apporter des réponses définitives à toutes ces questions. Au final, le transfert des données est une affaire de confiance. Et la confiance dépend de la simplicité, de la clarté et de la transparence avec lesquelles les conditions générales ainsi que les droits des personnes concernées sont présentés.

La sécurité absolue n'existe pas!
Les données les plus en sécurité sont celles qui ne sont jamais collectées ou, à certaines conditions, celles qui n'existent que chez vous sur papier ou qui ne sont pas sauvegardées de manière centralisée. Toutefois, il est aussi plus difficile de tirer parti de telles informations.

Conclusion: faut-il partager les données personnelles de santé avec la recherche scientifique?

Le conseil consultatif numérique répond à cette question par un «oui», à condition que les conditions-cadres soient claires et intelligibles pour les personnes concernées. Malgré tous les risques, les données peuvent être bénéfiques – à la société et parfois à soi-même. La recherche médicale, telle qu'elle est par exemple encadrée dans la loi relative à la recherche sur l'être humain, dispose de garde-fous relativement clairs, qui tiennent également compte de la protection des données et des droits individuels. Les règles ne sont pas parfaites, mais elles ont largement fait leurs preuves. Et elles s'appliquent également à la recherche industrielle (dès lors qu'une analyse relève de la «recherche médicale»).

Qui plus est, les scientifiques disposent d'une marge de manœuvre suffisante pour pouvoir eux-mêmes tenir compte des besoins et des souhaits des participants à l'étude en matière d'objectif, de transparence et d'implication, mais aussi de protection et de contrôle des données. Et il appartient à toutes les personnes impliquées de discuter des conditions-cadres, d'apporter des ajustements dans la mesure permise par la loi, mais aussi de communiquer de manière transparente et intelligible.

Les données sont une affaire de confiance − et la confiance doit se mériter.
D'ailleurs, la recherche n'a pour le moment pas accès au dossier électronique du patient.
Il n'existe encore aucune base légale pour cela.
