L'USINE NOUVELLE

PAYS :France
PAGE(S) :60,61
SURFACE :193 %
PERIODICITE :Hebdomadaire

RUBRIQUE :Guide
DIFFUSION :26554
JOURNALISTE :Sylvain Arnulf

► 29 septembre 2016 - N°3485

NUMÉRIQUE

Comment gérer les données de santé ?

Les entreprises doivent se préparer au nouveau règlement européen relatif aux données personnelles, qui entrera en vigueur en mai 2018.

SYLVAIN ARNULF

L'Europe a enfin réussi à bâtir un règlement unique concernant les données personnelles en général, et de santé en particulier. Il donne de nouveaux droits aux citoyens, de nouveaux devoirs aux entreprises et aux acteurs de la santé... et promet un peu moins de paperasse et de déclarations administratives.

1 SE RÉFÉRER À LA DÉFINITION EUROPÉENNE

Jusqu'à présent, la loi informatique et libertés de 1978 posait le principe d'un traitement des données relatives à la santé... sans pour autant les définir clairement. C'était la jurisprudence qui permettait d'en préciser les contours. Un règlement européen, publié en avril, après quatre ans d'âpres débats, et qui entrera en vigueur en mai 2018, en donne une définition plus claire. Il s'agit de « données à caractère personnel relatives à la santé mentale et physique d'une personne, y compris la prestation de services de soins de la santé qui révèle une information sur l'état de santé de la personne (...) présent, passé et futur ». Par donnée de santé, il faut entendre « toute information concernant 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 ». Les dispositifs connectés de contrôle du diabète, sur lesquels planchent actuellement Google et Sanofi, entrent dans ce cadre. Les données sont dites « personnelles » quand elles permettent d'identifier la personne concernée. C'est le cas des informations de remboursement de soins. « Nous les traitons comme des données de santé, car elles peuvent donner une indication sur l'état de santé du bénéficiaire », explique Jean-François Tripodi, le directeur général de Carte Blanche Partenaires, qui fait le lien entre réseaux de soins et mutuelles. Le fabricant d'objets connectés Withings, de son côté, héberge les données personnelles. Il les utilise pour ses projets de recherche « chez un tiers de confiance, pour qu'en aucun cas, nous ne puissions croiser les données », indique Alexis Normand, le directeur du Health Institute de la marque. S'il est aussi possible d'anonymiser ces données pour faciliter leur traitement en les supprimant, les masquant, ou en les agrégeant avec d'autres, l'anonymisation n'est pas infaillible et la réidentification est possible.

2 PAS DE DISTINCTION ENTRE BIEN-ÊTRE ET MÉDICAL

La nature du dispositif produisant la donnée n'induit pas un type de traitement. Un objet connecté grand public, de type bracelet d'activité, ou un dispositif médical, peuvent être soumis aux mêmes obligations. Tout comme un traitement manuel ou automatique, humain ou par une machine. C'est la finalité de l'utilisation des données qui importe. L'exploitation des données personnelles est interdite, mais le règlement prévoit une longue liste d'exceptions : entre autres, collecte dans le cadre de la mise en œuvre du droit social, de la sécurité sociale et de la protection sociale, « aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale ». Mais aussi pour des projets d'intérêt public qui peuvent concerner la recherche scientifique, des projets à des fins d'archivage historique, d'amélioration du système de santé... Comme l'exemple de Novartis ouvrant une plate-forme de partage de données, en collaboration avec le laboratoire La Paillasse, pour lancer un Challenge4Cancer, et combattre la maladie grâce au big data.

3 SÉCURISER L'HÉBERGEMENT DE DONNÉES SENSIBLES

En France, si le stockage des données de santé à caractère personnel est externalisé, il doit l'être chez un « hébergeur agréé ». Fin juin, près d'une centaine d'acteurs, établissements de santé, opérateurs télécoms et fournisseurs cloud étaient habilités à le faire. Ce stockage est évidemment plus coûteux que chez un hébergeur traditionnel. Il n'existe pas de règle précise concernant la durée de conservation des données. Celle-ci doit simplement être « pertinente par rapport à la finalité du traitement ». C'est au responsable de traitement de réfléchir à la bonne durée de conservation, ce qui lui laisse une certaine latitude. À lui aussi de savoir analyser les risques et de prendre les mesures appropriées pour assurer l'intégrité des données.

HERO IMAGES

CINQ BONS RÉFLEXES À ADOPTER

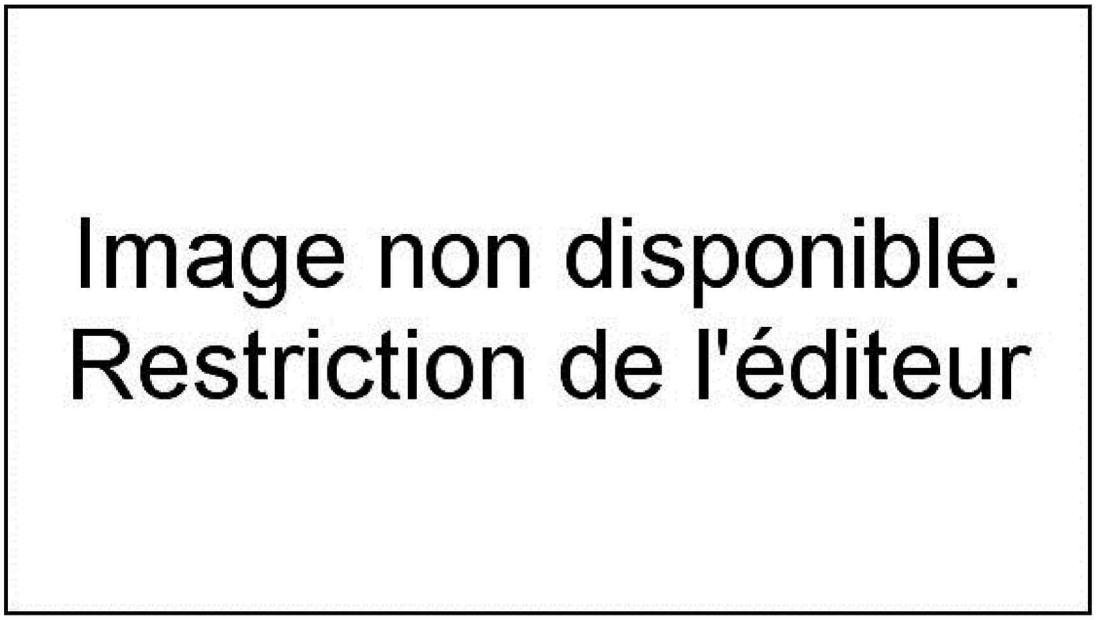
- **SUIVRE LE PRINCIPE** du « privacy by design » (protection des données dès la conception du produit ou du service et par défaut.
- **TRAVAILLER EN AMONT** avec la Commission nationale de l'informatique et des libertés (Cnil) pour mener une étude d'impact et adopter les bonnes pratiques.
- **SENSIBILISER** ses collaborateurs aux nouvelles réglementations.
- **ANONYMISER** les données sensibles au maximum.
- **ÊTRE TRANSPARENT** auprès du public pour faire du privacy by design un avantage concurrentiel.

L'USINE NOUVELLE

PAYS :France
PAGE(S) :60,61
SURFACE :193 %
PERIODICITE :Hebdomadaire

RUBRIQUE :Guide
DIFFUSION :26554
JOURNALISTE :Sylvain Arnulf

► 29 septembre 2016 - N°3485



Le règlement européen renforce les droits des personnes et responsabilise les acteurs traitant les données personnelles de santé.

4 DÉSIGNER DES CORESPONSABLES DE TRAITEMENT

La loi informatique et libertés prévoyait la désignation d'un « responsable de traitement », une personne morale, souvent le porteur de projet principal, qui traite les données en priorité. Celui-ci, en cas de traitement à grande échelle, devra désigner un ou plusieurs « délégués à la protection des données », une personne physique chargée de vérifier le respect des obligations légales, de faire le lien avec les différents acteurs, notamment les sous-traitants et la Commission nationale de l'informatique et des libertés (Cnil). 28 000 postes de data protection officers (DPO) devraient être créés en Europe dans les prochaines années. Le nouveau règlement européen instaure le principe d'une ouverture à des « responsables conjoints ». Ce dispositif permettra de traiter plus efficacement les « circulations de données complexes qui font intervenir différents acteurs, avec plusieurs niveaux de prestation », explique Thomas Duong, juriste au service santé au sein de la direction de la conformité de la Cnil. « Ce sera utile pour créer des services personnalisés », juge Jean-François Tripodi, de Carte Blanche Partenaires.

5 SUIVRE LES NOUVELLES OBLIGATIONS D'INFORMATION

Il est interdit d'utiliser les données personnelles d'un individu sans avoir obtenu son consentement explicite. Il doit avoir accès à une information « concise, aisément accessible, formulée en des termes clairs », quant à l'utilisation et au partage de ses données. Un droit à la portabilité des données est créé. Le règlement insiste sur la prévention, avec la nécessité d'une étude préalable des risques liés au traitement, et sur l'adoption du principe de protection des données dès la conception et par défaut. Le règlement introduit enfin une obligation de déclaration en cas de violation de données, en 72 heures maximum auprès de la Cnil, et « dans les meilleurs délais » auprès de la personne concernée. Les professionnels ont tout intérêt à jouer la transparence. Car « la première crainte des patients, c'est de voir leurs données perdues ou utilisées par des tiers », rappelle Éric Dessertene, le directeur business développement et commercial de Biocorp, une PME qui fabrique des dispositifs médicaux connectés. Ce nouveau règlement est une opportunité pour les rassurer... Et s'assurer un avantage concurrentiel.