DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Bases légales du DEP

Quo vadis?

La récente mise en consultation de la révision complète de la Loi fédérale sur le dossier électronique du patient (LDEP) a généré des interrogations protéiformes. Parmi elles, il en est une, récurrente, qui inquiète : cette révision signe-t-elle l'échec du dossier électronique du patient ? Cet article tente de répondre à cette question et d'envisager l'avenir avec un positivisme assumé, mais surtout un pragmatisme revendiqué.

Les chiffres publiés à la fin du mois d'août 2023 sont clairs : un peu plus de 25'000 DEP ont été ouverts, alors que l'objectif chiffré à atteindre à la fin de l'année 2022 était de 22'000 DEP.

Oui, le dossier électronique du patient est un échec cuisant!

Ni les professionnel·les de santé, ni les patient·es n'ont été convaincu·es par le projet, et ce pour différents motifs. Il apparaît clairement que les patient?es ignorent encore, pour la plupart, l'existence même du dossier électronique du patient. Seule une véritable évangélisation permettra de renverser la vapeur. A cela s'ajoute la complexité inhérente à l'ouverture d'un dossier. Il conviendrait donc d'aller à la rencontre des patient?es avec des guichets mobiles. A l'instar du « camion-Migros » de notre enfance, ces guichets pourraient essaimer le territoire cantonal avec des moyens didactiques, mais surtout comporter tout ce qui est nécessaire à la création immédiate du dossier électronique.

Quant aux professionnel-les de santé, le DEP leur génère un surcroît de travail, sans qu'ils n'en appréhendent encore tous les bénéfices actuels et futurs. En clair, les démarches visant à nourrir le dossier sont rébarbatives, chronophages et elles génèrent une frustration, car la plus-value n'est pas immédiatement perceptible s'agissant du suivi du/de la patient·e. Une simplification des processus doit être envisagée rapidement. Une intégration aux logiciels-métier des professionnel·les de santé est une nécessité absolue.

Et en termes de protection des données?

Notre système fédéraliste est poussé dans ses retranchements par un projet de ce type. Le Préposé fédéral et les préposés cantonaux peuvent être compétents à plusieurs titres et simultanément. Une coordination est donc nécessaire et celle-ci serait plus efficiente si la loi comportait des règles plus claires. Il s'agit du premier problème à résoudre et force est de constater qu'à ce jour, sans vouloir entrer dans les détails des efforts consentis, tout n'est pas encore réglé à satisfaction. A cela s'ajoutent les discrépances évidentes de ressources des préposés cantonaux qui, de manière générale et incontestable, ne disposent pas des moyens ni des ressources pour conduire des audits organisationnels ou de sécurité.

Les huit communautés de référence doivent certes diligenter leurs propres contrôles, mais cela n'est pas suffisant à l'aune du caractère sensible des données, mais surtout du fait que l'ensemble du système est fondé sur la confiance. Un seul piratage réussi et le DEP sera en grand danger. Mieux vaudrait certainement attribuer la compétence unique au Préposé fédéral à la protection des données et déroger ainsi au fédéralisme pour augmenter le niveau de maturité des systèmes d'information. Cela permettrait également d'éviter toute forme d'interactions des autorités ou des communautés dont la proximité avec les préposés cantonaux est plus intense. Le Préposé fédéral qui doit oeuvrer en bonne intelligence avec d'autres autorités fédérales (OFSP notamment) pourrait ainsi définir un cadre unique de régulation dont il s'assurerait du respect et de l'efficience.

Il est tout à fait possible, à l'instar de ce qui est survenu dans d'autres pays, que des problèmes graves soient générés par des sous-traitants notamment. Plus près de nous, ce qui est arrivé récemment à la société Medgate doit nous interpeller et nous inciter à une prudence de Sioux. Si le Préposé fédéral devait être désigné comme seul compétent pour vérifier la conformité aux normes en matière de protection des données, il pourrait prononcer des sanctions, ce qui sera impossible pour la plupart des préposés cantonaux. Ce seul motif suffit à exiger une reconsidération immédiate de la répartition des compétences de contrôle.

Accroître la sécurité des données auprès des professionnel-les de santé indépendant·es

Il existe également un pan négligé, à ce stade, de la sécurité des données. Si les hôpitaux, les cliniques et les cabinets de grande taille disposent des moyens pour accroître leurs défenses contre les attaques informatiques et la perte de données, il en va différemment des petits cabinets. Une consoeur américaine exposait, lors d'un congrès international, que le gouvernement avait financé la sécurité informatique des professionnel·les de santé à hauteur de plusieurs dizaines de milliers de dollars chacun. Le but était simple : empêcher des pirates informatiques d'accéder par leur intermédiaire à des structures de plus grande ampleur. Si nous voulons réellement protéger ces données sensibles, il conviendra à tout le moins d'offrir des ressources et de la connaissance à chaque maillon, surtout aux plus faibles. Et, à la connaissance du soussigné, cela n'est ni prévu ni envisagé. Le pragmatisme doit prévaloir et fournir aux professionnel-les de santé une cuirasse de défense pourrait déjà les convaincre de la minimisation du risque et leur permettre de se concentrer sur les bénéfices du projet.

En définitive, dans le champ de la protection des données, ce qui va permettre d'atteindre les objectifs fixés, c'est une simplification des processus de contrôle et un accroissement de la sécurité jusqu'aux prestataires les moins bien protégé·es. Cela concourra à accroître la confiance indispensable au succès.

Sébastien Fanti
Avocat