La protection des données du patient au défi de l'Espace européen des données de santé

Van Gyseghem, Jean-Marc; Degrave, Elise

Published in:
Espace européen des données de santé et IA

DOI:
10.4000/13vcw

Publication date:
2025

Document Version
le PDF de l'éditeur

La protection des données du patient au défi de l'Espace européen des données de santé – Échos de Belgique

Elise Degrave et **Jean-Marc Van Gyseghem**

p. 145-154

TEXTE INTÉGRAL

1 Initiative majeure de l'Union européenne, l'Espace européen des données de santé (EEDS) vise à organiser l'utilisation et la réutilisation des données de santé des patients au sein des États membres de l'Union tout en protégeant la confidentialité des données à caractère personnel, conformément au RGPD. Cela implique des particularités au niveau de la structure et du fonctionnement de pareil système.

2 Notre analyse se concentre dans un premier temps sur la structure organisationnelle de l'EEDS et le défi de la confiance des patients, en lien avec l'expérience belge qui se développe depuis plus de vingt ans. Dans un deuxième temps, on explique les balises qui encadrent l'utilisation et la réutilisation des données du patients dans les réseaux santé belges.

I. Décentraliser les données pour mieux les protéger

3 Un des objectifs de l'EEDS est de faciliter l'accès transfrontalier aux dossiers médicaux électroniques des patients qui se déplacent au sein de l'UE. Pour ce faire, les données médicales des citoyens européens ne sont pas centralisées en une seule base de données. Ce serait trop risqué en cas de cyber attaque par exemple, puisque l'accès à une seule base de données livrerait l'ensemble des données de chaque citoyen européen. C'est pourquoi, l'EEDS est fondé sur un modèle de décentralisation des données, qui consiste à maintenir les données dans le pays d'origine, et d'en organiser l'accès via des points de contact nationaux, pour permettre la réutilisation transfrontière de ces données.

§ 1. Le modèle de la décentralisation des données : la Belgique pionnière

4 En Belgique, dès les années 90, la volonté est née d'organiser une synergie entre les institutions publiques, de manière à ce que les données des citoyens puissent circuler entre elles. L'idée : permettre aux institutions publiques de ne pas devoir multiplier les demandes adressées aux personnes et faciliter la vie du citoyen qui ne doit plus communiquer dix fois son changement d'adresse, cette information pouvant circuler automatiquement.

5 Comme c'est le cas pour l'EEDS, le choix a été fait de décentraliser les données, c'est-à-

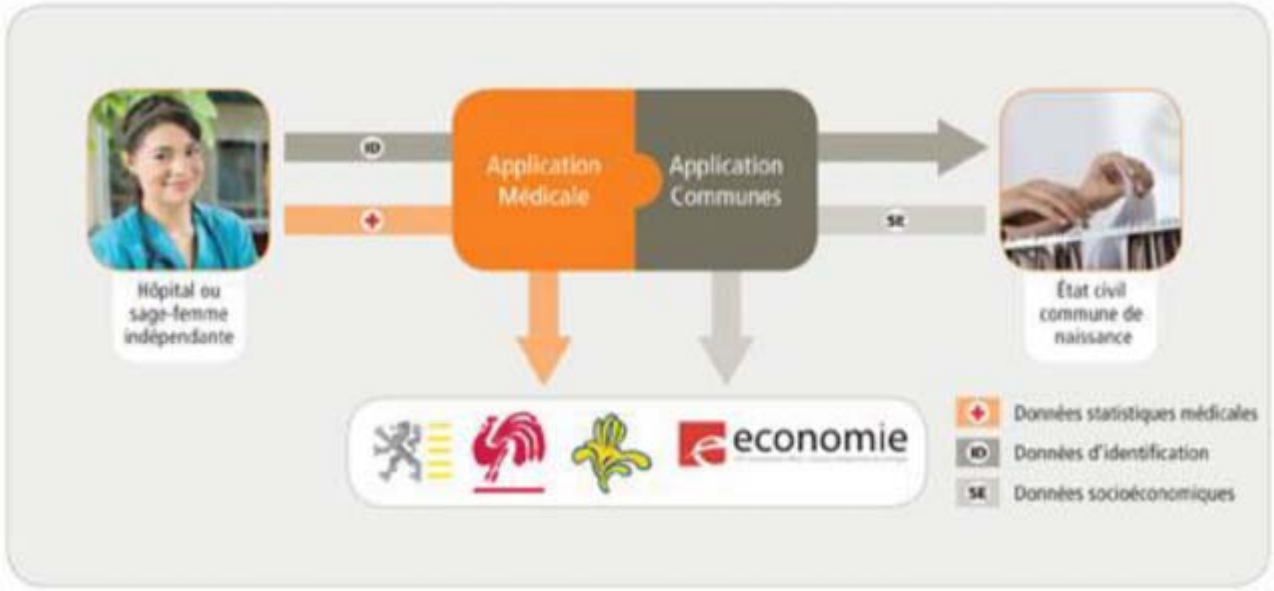
dire de « ne pas mettre tous les œufs dans le même panier ». C'est pourquoi, au niveau de l'État fédéral par exemple, les données d'identité sont enregistrées dans le Registre national, auprès du Service public fédéral Intérieur, les données fiscales sont enregistrées au Service public fédéral Finances, les données relatives à la pension sont enregistrées par le Service public fédéral pension, etc.

Si le Service public fédéral Finances a besoin de la nouvelle adresse d'un citoyen pour lui envoyer un document fiscal, il ne peut en principe plus demander cette information à la personne concernée. Il devra obtenir l'information directement du SPF Intérieur, grâce à une institution, appelée « intégrateur de services », ou « plateforme d'échanges d'information », qui est chargée de transmettre les informations d'une institution à une autre. En l'occurrence, il s'agira de l'intégrateur de services fédéral[1] qui organisera le cheminement de la donnée « nouvelle adresse » du SPF Intérieur vers le SPF Finances.

On constate là que la Belgique a devancé avant l'heure le fameux principe du « privacy by design » organisé par le RGPD[2], et qui consiste à intégrer la protection des données dans la structure même du système mis en place. C'est l'idée qu'en séparant les données et en les plaçant dans des bases de données différentes, on atteindra un niveau plus élevé de protection qu'en regroupant les données dans une base de données unique protégée par des mécanismes de sécurité informatiques. On peut raisonnablement penser que cette idée a convaincu le législateur européen d'opter pour la décentralisation des données dans la structure de l'EEDS.

En Belgique, en matière de santé, l'application « e-birth » illustre bien l'utilité du modèle de décentralisation des données et de la réutilisation de celles-ci permet aux hôpitaux d'envoyer l'attestation de naissance sous format électronique aux mairies, leur permettant d'enclencher rapidement les procédures administratives conséquentes à cet événement.

Schéma du fonctionnement de l'application e-birth[3]



§ 2. Le défi de la confiance du patient face à la réutilisation de ses données

La réutilisation des données du patient, en particulier de ses données à caractère personnel, ne peut se faire sans la confiance de chaque personne concernée, que ce soit au niveau national ou européen.

La confiance ne se décrète pas. Même un texte normatif irréprochable peut se heurter à la méfiance des citoyens. La confiance dans un système comme l'EEDS s'inspire. Elle doit se construire sur la base de plusieurs principes fondamentaux qui sous-tendent notamment le régime juridique de la protection des données à caractère personnel et que l'on retrouve dès lors dans le RGPD. On pointe ici les enjeux de transparence, de vie privée et d'égalité.

Tout d'abord, pas de confiance sans *transparence*. C'est la raison pour laquelle une attention soutenue doit être portée à l'accès par le patient à ses données à caractère personnel et à son droit d'obtenir une copie de son dossier médical. Nous y revenons dans la deuxième partie de cette étude.

Ensuite, la confiance suppose que chacun puisse être rassuré quant au fait qu'un système comme l'EEDS qui maximise la réutilisation des données de santé n'aboutira pas à une violation de sa *vie privée*. En particulier, il importe d'empêcher la réutilisation abusive de ces données par des personnes qui n'auraient pas le droit d'y accéder. À cet égard, en Belgique, un projet de loi porté par le Ministre de l'Économie en 2022 a créé l'émoi auprès de la population. Il était envisagé de transférer des données de santé, données à caractère personnel, à des sociétés d'assurance pour « assurer une meilleure efficience dans la gestion des contrats d'assurance »[4].

C'est pourquoi, il importe que la réutilisation des données de santé soit soumise à un contrôle rigoureux. À cet égard, l'article 51 du RGPD soumet les traitements de données au contrôle d'une « autorité de contrôle », incarnée par la CNIL, en France, et par l'Autorité de protection des données, en Belgique. Faut-il ajouter à cela des autorités propres aux traitements de données de santé ? C'est ce que la Belgique a jugé utile de faire. Deux institutions spécifiques ont été mises en place pour contrôler les données de santé : le Comité de sécurité de l'information et l'Agence des données de (soins de) santé[5].

De prime abord, l'existence d'autorités de contrôle spécialisées dans les données de santé est intéressante puisqu'on peut avoir confiance dans le fait que des spécialistes des données de santé vont examiner la légalité de ces échanges de données délicats. Néanmoins, l'expérience belge révèle que la multiplication de ces autorités en marge du travail du législateur pose problème. Ces deux autorités sont critiquées. En somme, il est reproché à ces autorités de rogner à la fois sur les compétences du législateur − seul compétent pour fixer le cadre légal entourant les traitements de données de santé − et sur les compétences de l'autorité de protection des données – seule

compétente pour exercer le contrôle organisé par le RGPD[6].

Enfin, on voit poindre le risque d'une médecine à deux vitesses, qui retient particulièrement notre attention dans ces lignes. La santé numérique ne risque-t-elle pas d'exclure une partie de la population de l'accès aux soins ? Or, santé doit rimer avec *égalité*. À cet égard, la Charte des droits fondamentaux de l'Union européenne affirme clairement que « toute personne a le droit d'accéder à la prévention en matière de santé et de bénéficier de soins médicaux dans les conditions établies par les législations et pratiques nationales. Un niveau élevé de protection de la santé humaine est assuré dans la définition et la mise en œuvre de toutes les politiques et actions de l'Union ».

Le numérique peut constituer un véritable frein à l'accès aux soins de santé. Cela peut être dû aux outils eux-mêmes, qui ne sont pas infaillibles. En cas de « bug », le patient est freiné dans sa démarche de soin. Plus encore, près d'un citoyen européen sur deux éprouve des difficultés pour accéder au numérique et/ou pour l'utiliser[7]. On constate par exemple que des personnes ne se soignent plus, car elles ne parviennent pas à prendre rendez-vous en ligne chez un médecin, et qu'elles ne se voient pas proposer d'alternative non numérique pour prendre rendez-vous[8]. Pour le dire autrement, la numérisation de la médecine peut créer de nouvelles discriminations, en particulier pour les personnes qui sont déjà vulnérables sur le plan socio-économique et se trouvent empêchées d'accéder aux soins, ce qui a pour effet d'exacerber encore davantage leur fragilité[9].

C'est pourquoi, cette situation fait réagir les autorités européennes.

Le Parlement européen, dans une résolution de 2022, souligne notamment « la nécessité de lutter contre la fracture numérique et l'exclusion financière des groupes sociaux vulnérables afin que la transformation numérique ne laisse personne de côté, en particulier ceux qui risquent le plus d'être dépourvus des compétences numériques dont ils ont besoin pour tirer le meilleur parti du potentiel de la numérisation des services publics et privés, afin de permettre l'inclusion de tous les citoyens dans la société numérique, indépendamment de leurs revenus, de leur situation sociale, de leur situation géographique, de leur santé ou de leur âge »[10].

Dans une recommandation de 2023, l'Assemblée parlementaire du Conseil de l'Europe « appelle les États membres et observateurs du Conseil de l'Europe (…) à considérer l'ensemble des politiques de lutte contre la fracture numérique comme une priorité »[11].

Par ailleurs, le Bureau régional de l'Organisation mondiale de la santé (OMS) a rendu, en 2023, un rapport qualifié d'« historique »[12] dans lequel il met en évidence qu'en Europe, seul un pays sur deux veille à renforcer les compétences numériques en santé[13].

S'agissant plus spécifiquement de l'Espace européen des données de santé, ce point

doit bien évidemment retenir l'attention. À cet égard, il est intéressant de constater que des organisations actives en matière de santé, comme la « European public health alliance »[14] réclament que des efforts plus importants soient consacrés à cette question affirmant notamment que « l'un des principaux objectifs du système EHDS [est] de permettre aux citoyens d'accéder en toute sécurité à leur dossier médical électronique, il est avant tout nécessaire de veiller à ce que tous les citoyens de l'UE aient accès à Internet et à d'autres technologies, telles que les smartphones, qui leur permettront d'utiliser leur dossier médical » et d'ajouter qu'il faudra aussi « veiller à ce que les citoyens soient suffisamment informés sur les outils numériques et la santé, le simple fait d'avoir accès à la technologie sans savoir comment l'utiliser ne permettra pas aux patients d'utiliser leur dossier médical électronique et de décider avec qui il sera partagé ». Gageons du fait que ces souhaits puissent être entendus.

II. Partager les données relatives à la santé au travers de l'Europe

Dans la suite de la crise de la Covid19, la Commission européenne a proposé le règlement sur l'Espace Européen des Données de Santé (EEDS) qui met en place deux niveaux de partage de données relatives à la santé au niveau européen, à savoir l'utilisation primaire et l'utilisation secondaire. Il s'agit, en quelque sorte, de la création d'une Union européenne de la santé[15].

Si le RGPD met la personne physique au centre de l'édifice de la protection des données et offre une *lex generalis*, l'EEDS se présente comme une *lex specialis*[16] en apportant un aspect sectoriel à la protection des données avec, d'une part, un volet individuel et, d'autre part, un volet d'intérêt public. L'on peut opérer un parallèle un peu audacieux entre la structure de l'article 8 de la Convention européenne des droits de l'Homme et l'EEDS en associant le caractère « individualiste » de l'alinéa 1 de l'article 8 avec l'utilisation primaire mise en place par l'EEDS et le caractère de « bien commun » de l'alinéa 2 de l'article 8 avec l'utilisation secondaire de l'EEDS.

Dans la présente contribution, nous allons analyser l'utilisation primaire qui doit conjuguer le partage de données entre professionnels de la santé dans le cadre de la prise en charge d'un patient et les droits que ce dernier aura sur ces mêmes données. Ainsi que cela a été énoncé ci-dessus, l'utilisation primaire met le patient est au cœur du partage avec, comme objectif majeur, faciliter l'accès et le partage des données de santé électroniques tant au niveau des professionnels de la santé que des patients eux-mêmes.

§ 1. Le partage de données entre professionnels de la santé

Le système mis en place par l'EEDS consiste en la création d'un dossier médical électronique (DME) structuré pour chaque patient. Grâce à ce DME et quel que soit l'État membre dans lequel il est établi, les professionnels s'inscrivant dans le suivi

médical du patient peuvent, d'une part, avoir accès aux informations concernant le patient − quel que soit l'État membre dans lequel il réside − et produites par d'autres professionnels de la santé et compléter, à leur tour, le DME en produisant des données. Ainsi, un médecin toulousain peut accéder au DME d'un patient belge hospitalisé à Toulouse et auquel il prodigue un suivi de soins de santé.

La Belgique connaît déjà et depuis de nombreuses années ce système de partage de données décentralisé par le biais des réseaux régionaux (hub) et d'une plateforme fédérale eHealth (metahub) qui permettent le partage de données de santé entre professionnels de la santé. Il est utile de relever que ce partage est possible sous la condition que tant le patient que le professionnel de soins de santé aient consenti au dit partage. L'exigence du consentement du patient devrait − alors même que l'EEDS institue un principe d'*opt out* − pouvoir être maintenue au regard du considérant 11 qui précise que le règlement « n'affecte pas les compétences des États membres en ce qui concerne l'enregistrement initial des données de santé électroniques à caractère personnel, telle que la soumission de l'enregistrement de données génétiques au consentement de la personne physique ou à d'autres garanties. (...) ».

Le partage de données dans le système belge est également tributaire de ce que le professionnel de la santé accepte de partager. Cette limite au partage devrait cependant disparaître par l'avènement de l'EEDS qui détermine les données auxquelles l'accès est fixé au travers de catégories prioritaires de données de santé électroniques à caractère personnel.

Dans le système des hubs et metahub belge, les professionnels de santé doivent avoir un lien thérapeutique pour pouvoir accéder aux données des patients outre le fait que cela soit dans un objectif de continuité des soins. Cette condition *sine qua non* exclut, entre autres, les médecins-conseils et les médecins-experts.

Ces exclusions paraissent être adoptées par l'EEDS à la lecture du considérant 19 qui précise que *« l'accès rapide et total des professionnels de la santé aux dossiers médicaux des patients est fondamental pour garantir* ***la continuité des soins****, éviter les duplications et les erreurs et réduire les coûts »*[17]. Il sera important de maintenir ce type d'exclusions afin de garantir la confiance du patient dans le système. En effet, le système mis en place par l'EEDS ne pourra pas fonctionner sans confiance du patient. Si ce dernier craint que l'accès aux données le concernant ne sera pas limité aux seuls professionnels de la santé impliqués dans la continuité des soins, il refusera l'utilisation primaire des dites données. Cela signera la fin de l'EEDS.

§ 2. Les droits du patient

Il est important de relever que les patients peuvent accéder aux données de santé les concernant[18] ainsi qu'« obtenir des informations, y compris au moyen de notifications automatiques, sur tout accès à leurs données de santé électroniques à caractère personnel obtenu par l'intermédiaire du service d'accès des professionnels de la santé

dans le cadre des soins de santé »[19]. Ce droit d'accès est distinct de celui prévu par l'article 15 du RGPD dès lors que « le droit d'accès aux données électroniques de santé à caractère personnel prévu par [l'EEDS] devrait, lui, être limité aux catégories de données entrant dans son champ d'application, être exercé par l'intermédiaire d'un service d'accès aux données électroniques de santé et donner lieu à une réponse immédiate ». Le patient pourra donc bénéficier d'un droit d'accès en vertu tant de l'EEDS que du RGPD. Par ailleurs, le patient dispose également d'un droit de rectification des données qui n'est cependant pas absolu. En effet, ce droit à rectification doit s'analyser au regard de l'article 16 du RGPD qui ne l'ouvre que si la donnée est inexacte ou incomplète. Il n'est donc pas question de permettre de demander la rectification de données qui ne lui « conviendraient » pas.

L'accès aux données peut être limité pour protéger la sécurité des patients et respecter la déontologie. Par exemple, l'accès peut être retardé jusqu'à ce qu'un professionnel de santé puisse communiquer les informations de manière appropriée. Cette limitation rappelle l'exception thérapeutique en droit belge, permettant de retarder l'accès si le patient n'est pas en mesure de recevoir l'information psychologiquement ; incapacité qui peut être temporaire et peut s'apparenter à un accompagnement particulier du patient lors de la communication de l'information. Cette situation se présente assez fréquemment dans des pathologies telles que le cancer pour lesquelles le médecin souhaite rencontrer le ou la patiente pour les prodiguer toutes les informations nécessaires et lui permettre d'appréhender la situation dans les meilleures conditions possibles avant le partage des informations via les réseaux.

Par ailleurs, les patients, dans le système belge, peuvent paramétrer l'accès à leurs données de manière granulaire au niveau tant des professionnels de la santé que des données elles-mêmes. En d'autres termes, ils peuvent exclure du partage des professionnels de la santé ou des données. L'EEDS devrait permettre à la Belgique de maintenir ce système de paramétrage des accès. L'on peut cependant s'interroger sur le maintien de la granularité des paramètres dès lors que l'article 8 précise que « les personnes physiques ont le droit de limiter l'accès des professionnels de la santé et des prestataires de soins de santé à tout ou partie de leurs données de santé électroniques à caractère personnel visées à l'article 3°». La question qui se pose est donc de savoir si la Belgique pourra maintenir un paramétrage au niveau du document ou de l'information ainsi que cela est actuellement le cas sur les réseaux santé. En effet, le patient peut paramétrer les accès au niveau du prestataire de soins de santé, mais également à celui du document/donnée. Il peut donc aller très loin dans son paramétrage. Les termes « à tout ou partie de leurs données » n'instaurent-ils donc pas un règlement européen moins favorable aux patients, car il permet moins de granularité. Va-t-on diminuer cette granularité propre au système belge pour se conformer au règlement ? Il nous semble que l'EEDS n'empêche pas un paramétrage plus fin que ce que le texte prévoit dès lors que le règlement impose des règles minimales qui pourraient être améliorées par les états membres à condition, bien

entendu, que cela ne porte pas atteinte aux objectifs visés par le règlement concerné. En l'espèce, une meilleure granularité dans les règles d'accès ou d'exclusion améliore l'autodétermination informationnelle du patient et, en conséquence, améliore l'approche visée par l'EEDS.

Conclusion

Le « réseau santé » européen est en route, et, au-delà des avantages offerts, devra prendre en compte les systèmes existants tel celui que la Belgique connaît, depuis de nombreuses années. L'EEDS ne pourra pas s'affranchir du respect du principe d'autodétermination informationnelle du patient.

Par ailleurs, il faudra veiller à ce que l'EEDS ne donne pas une raison – qui serait fallacieuse − pour l'État fédéral belge de s'approprier la coordination des autorités de santé. Cet appétit pourrait amoindrir, indirectement, les compétences des entités fédérées mais également provoquer une centralisation des traitements de données, centralisation qui s'avérerait un recul au niveau de la protection des données relatives à la santé des patients.

Ces questions devront nécessairement trouver des réponses, en veillant à ce que cela ne se fasse pas au détriment du patient et de la protection de sa vie privée au sens de l'article 8 de la Convention européenne des droits de l'Homme.

Notes de bas de page

1. Plus d'informations ici (dernière consultation le 15 novembre 2024) : https://bosa.belgium.be/fr/services/integrateur-de-services-federal.

2. Art. 25 RGPD.

3. Ce schéma provient de ce site : https://bosa.belgium.be/fr.

4. https://gcm.rmnet.be/clients/rmnet/content/medias/2021-09-08_projet_de_loi__donne__es_concernant_la_sante___rgpd__1_.pdf (dernière consultation le 15 novembre 2024). À cet égard, voy. E. Degrave, *L'État numérique et les droits humains,* Bruxelles, Académie royale de Belgique, 2024, pp. 12 et s.

5. Loi du 14 mars 2023 relative à l'institution et à l'organisation de l'Agence des données de (soins de) santé.

6. Voy. not. à propos de l'Agence des données de (soins de) santé, l'avis de l'Autorité de protection des données, avis n° 234/2022 du 29 septembre 2022 et Projet de loi relatif à l'institution et à l'organisation de l'Agence des données de (soins de) santé, Rapport de la deuxième lecture fait au nom de la commission de la Santé et de l'Égalité des chances par M. Daniel Bacquelaine, *Doc. Parl.,* Ch. repr., session 2022-2023, doc 55 3065/007.

7. Le chiffre de 56 % de personnes ayant les compétences de base en numérique était avancé en 2022 ; Cfr Résolution du Parlement européen du 13 décembre 2022 sur la fracture numérique : les différences sociales produites par la numérisation (voy. Point I.), accessible ici : https://www.europarl.europa.eu/doceo/document/TA-9-2022-0438_FR.html. La Commission avance désormais le chiffre de 55,6 % (Communique « Digital skills » accessible ici : https://digital-strategy.ec.europa.eu/en/policies/digital-skills.

8. Information communiquée par une association de lutte contre l'analphabétisme au colloque « IA et inégalités sociales » organisé par le centre de recherches OBVIA à Montréal les 31 octobre et 1er novembre 2024.

9. J. A. Greene *The Doctor Who Wasn't There: Technology, History, and the Limits of Telehealth*. Chicago, University of Chicago Press, 2022 cité par M. Al Dahdah et V. Duclos, "Santé numérique. Transformations sociotechniques du soin et des pratiques de santé dans un monde connecté », *Anthropologie & Santé,* 2024, n° 15, accessible ici : https://journals.openedition.org/anthropologiesante/13648

10. Résolution du Parlement européen du 13 décembre 2022, précitée.

11. Assemblée parlementaire du Conseil de l'Europe, « Réduire la fracture numérique : promouvoir l'égalité d'accès aux technologies numériques », Résolution 2510 (2023), accessible ici : https://pace.coe.int/fr/files/33001/html (dernière consultation : 15 novembre 2024).

12. https://www.who.int/europe/fr/news/item/05-09-2023-digital-health-divide--only-1-in-2-countries-in-europe-and-central-asia-have-policies-to-improve-digital-health-literacy--leaving-millions-behind

13. Voy. Bureau régional de l'OMS, «The ongoing journey to commitment and transformation Digital health in the WHO Eu », 5 septembre 2023, p. 9 accessible ici : https://cdn.who.int/media/docs/librariesprovider2/data-and-evidence/english-ddh-260823_7amcet.pdf?sfvrsn=4c674522_2&download=true (dernière consultation le 15 novembre 2024).

14. https://epha.org/digital-skills-for-all/ (dernière consultation : 15 novembre 2024).

15. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_fr

16. Ainsi, l'article 1, 2, a) du règlement établit clairement que le règlement « précise et complète les droits conférés par le [RGPD] aux personnes physiques en ce qui concerne l'utilisation primaire et secondaire de leurs données de santé électroniques à caractère personnel ».

17. Nous soulignons.

18. Art. 3 du règlement.

19. Art. 9.1 du règlement.

Auteurs

Elise Degrave

Professeure à la Faculté de droit de l'Université de Namur, Co-directrice de la Chaire E-gouvernement de l'Université de Namur et chercheuse au Nadi/Crids

Jean-Marc Van Gyseghem

Directeur adjoint du Centre de recherches Information, Droit et Société (Crids) de l'Université de Namur