Agence des données de (soins de) santé (ADS)

Analyse juridique du cadre légal applicable aux flux de données de santé

Agenda/Topics

- Réglementation applicable au traitement secondaire des données personnelles et de santé
  - Cadre Européen
  - Réglementation Nationale
- Autorités de contrôle
- Les flux de données et leurs réglementations applicables

Réglementation applicable au traitement secondaire des données personnelles et de (soins) santé - Introduction (1/4)

- **Introduction : traitement primaire et traitement secondaire des donnés de santé (1/2):**

L'ADS veut jouer un rôle de facilitateur dans l'accès aux données de (soins de) santé pour le traitement secondaire. Le contenu de la notion de **traitement « primaire » des soins de santé et du traitement « secondaire » des soins de santé** varie d'un texte réglementaire à l'autre.

1° Le RGPD (Règlement général sur la protection des données) ne prévoit pas de description spécifique du traitement primaire et du traitement secondaire des données personnelles. Nous pouvons en référer à l'article 5, alinéa 1 du RGPD. Il dispose que les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes. Les données ne peuvent pas être traitées ultérieurement (« traitement secondaire ») d'une manière incompatible avec ces finalités. Le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1 du RGPD, comme incompatible avec les finalités initiales.

Réglementation applicable au traitement secondaire des données personnelles et de (soins) santé - Introduction (2/4)

- **Introduction : traitement primaire et traitement secondaire des donnés de santé (2/2)** :

2° La **proposition de Règlement EHDS** applique les définitions suivantes (lesquelles sont bien plus strictes, l'utilisation primaire se concentrant en premier lieu sur le traitement des données de santé pour la fourniture et le paiement de soins de santé) :

- « utilisation primaire des données de santé électroniques » : le traitement de données de santé électroniques pour la fourniture de services de santé visant à évaluer, maintenir ou rétablir l'état de santé de la personne physique à laquelle ces données se rapportent, y compris la prescription, la dispensation et la fourniture de médicaments et de dispositifs médicaux, ainsi que pour les services de sécurité sociale, administratifs ou de remboursement pertinents ;

- « utilisation secondaire des données de santé électroniques » : le traitement de données de santé électroniques aux fins énoncées au chapitre IV dudit règlement. Les données utilisées peuvent inclure des données de santé électroniques à caractère personnel initialement collectées dans le cadre d'une utilisation primaire, mais aussi des données de santé électroniques collectées en application du chapitre IV dudit règlement.

3° En vertu de **la loi ADS,** la réutilisation des données de (soins de) santé est complétée comme suit : *« l'utilisation par des personnes physiques ou morales de données, dont les détenteurs de données disposent, à des fins commerciales ou non commerciales, autres que l'objectif initial pour lequel les données sont traitées, à l'exception de l'échange de données entre organismes publics prescrit par la loi »*.

Réglementation applicable au traitement secondaire des données personnelles et de santé - Introduction (3/4)

- **Données pseudonymisées, synthetic data et données anonymisées (1/2):**

1° **Les données pseudonymisées** ne sont pas des données anonymes, étant donné qu'elles permettent toujours d'identifier la personne concernée au moyen d'une clé. La pseudonymisation est définie dans le RGPD comme suit :

« *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable*. »

En outre, le considérant 26 du RGPD indique ce qui suit :

"Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci »

Réglementation applicable au traitement secondaire des données personnelles et de santé - Introduction (4/4)

- **Données pseudonymisées, synthetic data et données anonymisées (2/2):**

2° Les données anonymisées impliquent que les personnes concernées ne peuvent pas être identifiées par une personne de quelque manière que ce soit. Le considérant 26 du RGPD définit les données anonymes comme suit :

« Les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable."

En ce qui concerne l'anonymisation et la pseudonymisation des données personnelles, il convient de se référer également aux articles 198 à 204 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

3° Enfin, le concept de génération de données synthétiques consiste à prendre une source de données originale (set de données) et à créer à partir de celle-ci de nouvelles données artificielles présentant des propriétés statistiques similaires. La préservation des propriétés statistiques signifie que toute personne analysant les données synthétiques, par exemple un analyste de données, devrait être en mesure de tirer les mêmes conclusions statistiques de l'analyse d'un ensemble donné de données synthétiques que si on lui fournissait les données réelles (originales)

Réglementation applicable au traitement secondaire des données personnelles et de santé - Cadre européen (1/10)

- **RGPD (1/2)**

Traitement secondaire des données de santé en vertu du RGPD

a. Données de santé comme données personnelles particulières

Le traitement des **données sur la santé** est qualifié de traitement de **données personnelles particulières**.

Le considérant 4 du RGPD définit la notion de « données concernant la santé » comme suit : « *données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ». Le considérant 35 du RGPD indique qu'il convient d'interpréter largement la notion de données concernant la santé.

b. Traitement licite des données relatives à la santé : base juridique du traitement

Les données doivent être traitées de manière licite, appropriée et transparente.

Le traitement des données relatives à la santé est fondamentalement interdit. Ces données ne peuvent être traitées qu'en vertu de l'un des motifs d'exception spécifiques prévus à l'**article 9, paragraphe 2, RGPD**, à savoir le consentement explicite, les obligations et les droits en matière de droit du travail, de la sécurité sociale et de la protection sociale, la sauvegarde des intérêts vitaux, les dossiers d'adhésion d'associations ou de fondations en rapport avec l'exercice des libertés fondamentales, les données personnelles manifestement rendues publiques, l'institution, l'exercice ou le soutien d'une action en justice, les raisons d'intérêt prépondérant, les diverses fins de soins de santé, les droits de santé publique et l'archivage dans l'intérêt public, la recherche scientifique ou historique ou les fins statistiques.

Règlementation applicable au traitement secondaire de données personnelles et de données de (soins de) santé - Cadre européen (2/10)

- **RGPD (2/2)**

Le **consentement** est défini comme une expression de volonté qui doit être non équivoque, explicite et qui doit se manifester soit par une déclaration, soit par un acte actif non équivoque. Un consentement est explicite s'il se traduit par une expression explicite de la volonté. Ce consentement explicite peut être retiré à tout moment. Ce retrait ne peut qu'avoir des conséquences pour l'avenir. Il peut également recouru à la protection d'**intérêts vitaux** ou à des **raisons impérieuses**.

Du reste, l'article 9, alinéa 2 du RGPD émet l'exception suivante : *« le traitement est nécessaire **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** , sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3* »

Est par ailleurs pertinente l'exception qui permet de traiter ces données de santé aux motifs de **d'intérêt public dans le domaine de la santé publique**. Il s'agit notamment de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, et en particulier le secret professionnel. Le traitement de données personnelles aux motifs de l'intérêt général ne peut pas conduire au traitement de ces données personnelles par des compagnies d'assurances à d'autres fins.

Enfin, le **traitement à des fins statistiques** peut également se révéler pertinent. Ce traitement doit satisfaire à la règlementation visée à l'article 89, alinéa 1er du RGPD.

Règlementation applicable au traitement secondaire de données personnelles et de données de (soins de) santé - Cadre européen (3/10)

- **Proposition de Règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé (ci-après : Règlement EHDS)**

Le 3 mai 2022, **une proposition de** Règlement EHDS a été déposée. Celle-ci présente l'objet général suivant :

« que les personnes physiques aient davantage de contrôle sur leurs données de santé électroniques, *il s'agit aussi de garantir un cadre juridique consistant en des mécanismes de gouvernance fiables et en un environnement de traitement sécurisé, il s'agit également de contribuer à un véritable marché unique des produits et services de santé numérique, en harmonisant les règles de manière à renforcer l'efficience des services de santé »*

Le Règlement EHDS (bien qu'il ne soit pas encore fonctionnel) accorde une importance toute particulière à l'utilisation secondaire des données de santé électroniques. Le Règlement EHDS s'appuie sur la proposition de règlement relatif à la gouvernance des données.

Le règlement relatif à la gouvernance des donnés ne fait que fixer des conditions générales pour l'utilisation secondaire des données publiques, sans réellement créer un droit à l'utilisation secondaire de ces données. La proposition de règlement sur les données renforce la portabilité de certaines données générées par les utilisateurs, qui peuvent inclure des données de santé, mais ne renferme pas de règles pour toutes les données de santé. C'est pourquoi l'EHDS vient s'ajouter à ces propositions d'actes législatifs et entend des règles plus spécifiques pour le secteur de la santé. Ces règles spécifiques concernent l'échange de données de santé électroniques et peuvent affecter les prestataires de services d'échange de données, les formats par lesquels la portabilité des données de santé est assurée, les règles de coopération pour l'altruisme en matière de données dans le domaine de la santé et la complémentarité relativement à l'accès aux données privées pour une utilisation secondaire.

Le tableau du rapport circonstancié analyse ces éléments du règlement EHDS particulièrement pertinent pour l'ADS (lien).

Règlementation applicable au traitement secondaire de données personnelles et de données de (soins de) santé - Cadre européen (4/10)

- **Règlement portant sur la gouvernance des donnés (Règlement UE 2022/868 du Parlement européen et du Conseil portant sur la gouvernance européenne des données) (1/3)**

Le Règlement sur la gouvernance des données est un règlement européen pour la gestion des données. Le règlement prévoit les priorités suivantes:

- Faciliter la réutilisation des informations publiques ;
- Obligations pour les fournisseurs de données : ceux-ci doivent faire preuve de transparence et œuvrer en toute neutralité ;
- La stimulation du partage altruiste de données ;
- La désignation d'un « *comité européen de l'innovation dans le domaine des données* ». Ce groupe d'experts veille à l'utilisation du Règlement dans l'UE et émet des avis.

Le Règlement relatif à la gouvernance des données ne porte pas préjudice aux dispositions du RGPD. Du reste, la règlementation sectorielle prévaut, ce qui signifie que le Règlement EHDS prévaut dès son adoption.

Les éléments suivants figurant au Règlement relatif à la gouvernance des données sont particulièrement pertinents pour l'ADS et le développement des missions de l'ADS :

- Les conditions en matière de réutilisation des données ;
- Les redevances par rapport à cette réutilisation de données ;
- Les organes compétents ;
- Le service d'intermédiation de données et;
- L'altruisme en matière de données.

Réglementation applicable au traitement secondaire des données personnelles et de santé - Cadre européen (5/10)

- **Règlement sur la gouvernance des données (Règlement UE 2022/868 du Parlement européen et du Conseil sur la gouvernance européenne des données) (2/3)**

a) Conditions applicables à la réutilisation de données

Les organismes du secteur public ont le pouvoir d'accorder ou de refuser l'accès à certaines catégories de données à des fins de réutilisation et sont tenus de rendre publiques les conditions permettant une telle réutilisation et la procédure d'autorisation de la réutilisation. Les conditions de réutilisation doivent être non discriminatoires, transparentes, proportionnées et justifiées objectivement en ce qui concerne les catégories de données, l'objectif de la réutilisation et la nature des données pour lesquels la réutilisation est permise.

Le considérant 2 du règlement sur la gouvernance des données donne plus d'explications à ce sujet :

*"**Les espaces européens communs de données devraient rendre les données traçables, accessibles, interopérables et réutilisables (ci-après dénommé «principes FAIR pour les données»), tout en garantissant un niveau élevé de cybersécurité. Lorsqu'il existe des conditions de concurrence équitables dans l'économie des données, les entreprises se font concurrence sur la qualité des services, et non sur la quantité de données qu'elles contrôlent**. […]"*

Les principes énoncés dans le règlement sur la gouvernance des données sont pertinents pour la mise en œuvre de diverses missions de l'ADS:
« Art. 5. § 1. L' Agence des données de (soins de) santé est chargée des missions suivantes en vue de l'exécution de son objectif:
[…]
*2° **Assumer un rôle de facilitateur dans les demandes d'accès aux données de (soins de) santé et des données relatives à la (aux soins de) santé**;*
*3° **Documenter et optimaliser les processus de demandes de réutilisation de données de (soins de) santé et des données relatives à la (aux soins de) santé**;*
*4° **Mettre en place un modèle de gouvernance transparent et efficace pour la réutilisation des données de (soins de) santé et des données relatives à la (aux soins de) santé** »*

Règlementation applicable au traitement secondaire de données personnelles et de données de (soins de) santé - Cadre européen (6/10)

- **Règlement sur la gouvernance des donnés (Règlement UE 2022/868 du Parlement européen et du Conseil portant sur la gouvernance européenne des données) (3/3)**

Le Règlement sur la gouvernance des données prévoit du reste que les organismes du secteur public soient tenus de s'assurer que le caractère protégé des données demeure immuable.

Enfin, les prestataires de services d'intermédiation de données doivent pouvoir fournir aux détenteurs de données ou aux personnes concernées des outils et services spécifiques supplémentaires visant spécifiquement à faciliter l'échange de données, tels que le stockage temporaire, l'organisation, la conversion, l'anonymisation et la pseudonymisation.

(b) Les redevances pour la réutilisation de données.

Les organismes du secteur public qui donnent leur consentement à la réutilisation de certaines catégories de donnés peuvent demander une redevance. Les redevances sont transparentes, non discriminatoires, proportionnées et objectivement justifiées et ne restreignent pas la concurrence. Les redevances sont calculées sur la base des coûts liés à la conduite de la procédure de demande de réutilisation des catégories de données et limitées aux coûts nécessaires relatifs :

- à la reproduction, à la fourniture et à la diffusion des données ;
- à l'acquisition des droits ;
- à l'anonymisation ou à d'autres formes de préparation des données à caractère personnel et des données commerciales confidentielles ;
- à la maintenance de l'environnement de traitement sécurisé ;
- à l'acquisition du droit d'autoriser la réutilisation conformément au présent chapitre par des tiers extérieurs au secteur public; et
- à l'assistance fournie aux réutilisateurs pour obtenir le consentement des personnes concernées et l'autorisation des détenteurs de données dont les droits et intérêts peuvent être affectés par cette réutilisation.

Les critères et la méthode de calcul des redevances sont arrêtés par les États membres et publiés.

Réglementation applicable au traitement secondaire des données personnelles et de santé - Cadre européen (7/10)

- **Règlement (UE) n° 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE (règlement de l'UE sur les essais cliniques) (1/2)**

Le règlement européen sur les essais cliniques prévoit un degré élevé d'harmonisation des règles relatives à la conduite des essais cliniques dans l'UE. Le règlement introduit :

- une procédure d'autorisation basée sur une soumission unique via un portail européen unique ;
- une procédure d'évaluation aboutissant à une décision unique ;
- les règles relatives à la protection des sujets et au consentement éclairé ; et
- les exigences de transparence.

Il sera également plus facile pour les entreprises pharmaceutiques de mener des essais cliniques multinationaux, ce qui devrait augmenter le nombre d'études réalisées dans l'UE.

(a) Portail de l'UE et base de données des essais cliniques de l'UE

Le règlement charge l'Agence européenne des médicaments d'établir un portail européen et une base de données européenne. Le portail de l'UE sera le point central pour la soumission des données d'essais cliniques et des informations requises par le règlement. La base de données de l'UE contiendra toutes les données et informations soumises via le portail de l'UE.

Réglementation applicable au traitement secondaire des données personnelles et de santé - Cadre européen (8/10)

- **Règlement (UE) n° 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE (règlement de l'UE sur les essais cliniques) (2/2)**

(b) Transparence

Le règlement sur les essais cliniques assure une plus grande transparence des données relatives aux essais cliniques. Toutes les informations contenues dans la base de données de l'UE seront accessibles au public, sauf si leur confidentialité peut être justifiée pour des raisons de :

- protection des informations commercialement confidentielles ;
- protection des données personnelles ;
- protection des communications confidentielles entre les pays de l'UE ;
- assurer une supervision efficace de la conduite des essais cliniques par les pays de l'UE.

Règlementation applicable au traitement secondaire de données personnelles et de données de (soins de) santé - Cadre européen (9/10)

- **Services électroniques pour les soins de santé transfrontaliers (1/2)**

À l'échelle européenne, l'infrastructure de services numériques pour la santé en ligne (eHDSI) constitue une infrastructure garante de soins de santé sur lesquels les citoyens européens peuvent compter lorsqu'ils se rendent dans un autre pays de l'UE. Elle permet aux pays de l'UE d'échanger des données de santé de manière sûre, efficace et interopérable. Grâce au logo « **MyHealth@EU** », les citoyens peuvent connaître la disponibilité de ces services à un endroit en particulier.

Les États membres s'affairent actuellement à l'introduction de deux services électroniques transfrontaliers :

- La **prescription et la délivrance électroniques de médicaments** : Les citoyens européens pourront retirer leurs médicaments dans une pharmacie d'un autre pays de l'UE, puisque la prescription peut être transmise en ligne dans un autre pays ;

- Le **dossier électronique élémentaire du patient** : il renferme des informations de santé importantes, (par exemple concernant des allergies, des traitements en cours, des maladies antérieures, des opérations, etc.) et fait partie du dossier électronique du patient plus exhaustif. Le dossier électronique élémentaire du patient donne aux médecins des informations essentielles à propos d'un patient, dans sa propre langue, lorsqu'un patient d'un autre pays de l'UE arrive et qu'il y a un problème d'ordre linguistique.

À terme, **les imageries médicales et les résultats d'analyses** devront également être disponibles dans toute l'UE, pour en arriver en définitive au **dossier médical global**. Tous les pays de l'UE doivent coopérer à l'échange des prescriptions électroniques et des dossiers électroniques élémentaires des patients.

Règlementation applicable au traitement secondaire de données personnelles et de données de (soins de) santé - Cadre européen (10/10)

- **Services électroniques pour les soins de santé transfrontaliers (2/2)**

En ce qui concerne la **prescription et la délivrance électroniques de médicaments**, les États membres du réseau de santé en ligne ont approuvé des clauses complémentaires aux directives générales pour l'échange électronique de données de santé dans le cadre de la Directive 2011/24/UE et du Règlement d'exécution 2021/52/UE afin de soutenir l'échange de données sur les prescriptions électroniques et leur délivrance. Ces lignes directrices ajoutent des orientations spécifiques et complètent les lignes directrices générales du réseau de santé en ligne. Le **dossier électronique élémentaire du patient** s'inscrit dans le cadre d'un cas d'utilisation qui représente un degré élevé de consensus sur les services européens de e-santé. Ce cas d'utilisation est décrit dans la Directive 2011/24/UE du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers.

Réglementation traitement secondaire des données personnelles et de santé - Réglementation nationale (1/2)

- **Loi de 2018 sur le traitement des données à caractère personnel**

L'article 9 de la loi de 2018 sur le traitement des données personnelles prévoit :

“En exécution de l'article 9.4 du Règlement, le responsable du traitement prend les mesures supplémentaires suivantes lors du traitement de données génétiques, biométriques ou des données concernant la santé :

1° les catégories de personnes ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;

2° la liste des catégories des personnes ainsi désignées est tenue à la disposition de l'autorité de contrôle compétente par le responsable du traitement ou, le cas échéant, par le sous-traitant;

3° il veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées. »

En ce qui concerne le traitement secondaire des données personnelles, il convient également de se référer aux articles 194 à 197 de la loi. En particulier, l'article 197 dispose :

"Le responsable du traitement à des fins de recherche ou statistiques utilise des données anonymes.

Lorsqu'un traitement de données anonymes ne permet pas d'atteindre la finalité de la recherche ou statistique, le responsable du traitement utilise des données pseudonymisées.

Lorsqu'un traitement de données pseudonymisées ne permet pas d'atteindre la finalité de recherche ou statistique, le responsable du traitement utilise des données non-pseudonymisées. »

Réglementation traitement secondaire des données personnelles et de santé - Réglementation nationale (2/2)

- **Loi relative aux droits du patient**

L'article 10 de la loi du 22 août 2002 concernant les droits du patient se révèle plutôt pertinente. Celui-ci dispose que :

> *« § 1. Le patient a droit à la protection de sa vie privée lors de toute intervention du praticien professionnel, notamment en ce qui concerne les informations liées à sa santé.*
> *Le patient a droit au respect de son intimité. Sauf accord du patient, seules les personnes dont la présence est justifiée dans le cadre de services dispensés par un praticien professionnel peuvent assister aux soins, examens et traitements.*
> *§ 2. Aucune ingérence n'est autorisée dans l'exercice de ce droit sauf si cela est prévu par la loi et est nécessaire pour la protection de la santé publique ou pour la protection des droits et des libertés de tiers.*

- **Loi relative à la qualité de la pratique des soins de santé**

La section 12 de la loi relative à la qualité de la pratique des soins de santé régit uniquement l'accès aux données de santé par les professionnels de soins de santé. Il s'en dégage que les personnes qui ne sont pas des professionnels de soins de santé en vertu de la loi relative à la qualité de la pratique des soins de santé n'ont pas accès aux données de santé du patient. Une autre base juridique doit le prévoir. Le professionnel de soins de santé a accès aux données à caractère personnel relatives à la santé du patient qui sont tenues à jour et conservées par d'autres professionnels des soins de santé à condition que le patient ait préalablement donné son consentement éclairé audit accès. L'article 9, paragraphe 2, point 3, de la loi relative aux droits du patient prévoit également un arrangement selon lequel un professionnel de soins de santé a « accès » dans des conditions très strictes aux données personnelles relatives à la santé d'un patient qui n'est pas « son » patient.

La loi relative à la qualité de la pratique des soins de santé ne contient aucune disposition relative au refus ou au retrait du consentement à l'accès aux données de santé d'un patient. Le Conseil d'État a estimé que cette disposition n'était pas nécessaire étant donné qu'elle est prévue par le RGPD, qui est directement applicable dans le cadre du droit national.

Autorités de contrôle (1/6)

- **Autorité de protection des données (1/2)**

L'Autorité de protection des données (APD) est un organe indépendant qui veille au respect des principes fondamentaux de la protection des données personnelles. L'Autorité de protection des données est dotée de diverses compétences, notamment :

- Un contrôle du respect des principes fondamentaux de la protection des données personnelles ;
- Un **centre de connaissances** compétent pour émettre des avis sur toutes les questions relatives aux traitements des données à caractère personnel. Ce centre de connaissances est également habilité à formuler des recommandations relatives aux développements sociétaux, économiques et technologiques qui peuvent avoir une incidence sur les traitements de données à caractère personnel ;
- Un **service d'inspection** qui chapeaute des enquêtes sur les plaintes et les indices sérieux de violation de la législation sur les données à caractère personnel ;
- Une **chambre contentieuse** compétente pour faire appliquer les règles dans les affaires saisies ou basées sur une inspection de sa propre initiative ;
- Un **service de première ligne** compétent pour réceptionner les plaintes, faire office d'intermédiaire, informer le citoyen, sensibiliser.
- **Autorité de protection des données.**

<u>Relation entre l'APD et l'ADS</u>

L'ADS n'est pas une autorité de contrôle au sens de l'article 51 du RGPD. L'exposé des motifs prévoit en outre que l'ADS ne vise pas à remplacer l'APD ni à porter atteinte à ses pouvoirs. L'ADS vise à jouer un **rôle de facilitateur de l'accès aux données de (soins de) santé pour le traitement secondaire**.

S'il est question de donner des conseils dans les projets de textes de l'ADS, cela doit être interprété dans le sens d'un "soutien" et non d'un conseil juridiquement requis ou d'une obligation légale de continuer à utiliser ce conseil.

Le demandeur de données doit avoir une base légale pour sa demande de données (sur laquelle un avis de l'APD doit être disponible s'il s'agit de données à caractère personnel, et doit obtenir une délibération (positive) du CSI.

Autorités de contrôle (2/6)

- **Autorité de protection des données (1/2)**

Relation entre l'APD et l'ADS

L'ADS n'est pas une autorité de contrôle au sens de l'article 51 du RGPD. L'exposé des motifs prévoit en outre que l'ADS ne vise pas à remplacer l'APD ni à porter atteinte à ses pouvoirs. L'ADS vise à jouer un **rôle de facilitateur de l'accès aux données de (soins de) santé pour le traitement secondaire**.

S'il est question de donner des conseils dans les projets de textes de l'ADS, cela doit être interprété dans le sens d'un "soutien" et non d'un conseil juridiquement requis ou d'une obligation légale de continuer à utiliser ce conseil.

Le demandeur de données doit avoir une base légale pour sa demande de données (sur laquelle un avis de l'APD doit être disponible s'il s'agit de données à caractère personnel, et doit obtenir une délibération (positive) du CSI.

Autorités de contrôle (3/6)

- **Comité de sécurité de l'information**

Compétence du CSI d'accorder des autorisations pour l'utilisation secondaire de données personnelles (1/2)

Le CSI comprend deux chambres (la chambre « Sécurité sociale et Santé » et la chambre « Autorité fédérale ») et se compose de membres désignés par la Chambre des représentants. Les demandes d'accès aux données de (soins de) santé sont soumises à la Chambre Sécurité sociale et Santé du CSI pour délibération en vue de l'obtention d'une autorisation. Cette chambre vérifie notamment la satisfaction des conditions de limitation des finalités, de proportionnalité et de sécurité fixées dans le RGPD.

En ce qui concerne l'obtention d'autorisations par le CSI, il convient de distinguer, en fonction de la nature ou du contenu des données, les données personnelles sociales d'une part et les données relatives à la santé (soins) d'autre part.

Le 22 septembre 2022, la Cour constitutionnelle a jugé que la législation sur le traçage manuel et numérique des contacts pour lutter contre le COVID-19 est constitutionnelle, sauf sur trois points. L'un de ces points concerne l'autorisation du CSI de permettre la communication de données personnelles à des tiers. Plus précisément, les parties requérantes critiquaient l'habilitation conférée au Comité de sécurité de l'information d'autoriser la communication à des tiers des données à caractère personnel pseudonymisées enregistrées dans la base de données à des fins de recherche scientifique. A cet égard, la Cour rappelle que l'article 22 de la Constitution réserve au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée et familiale. Une habilitation à un autre pouvoir est cependant admissible, pour autant qu'elle soit définie de manière suffisamment précise et que le législateur ait lui-même fixé les éléments essentiels. La Cour relève que le CSI est un organe qui est indépendant de l'APD et qui a été créé par une loi du 5 septembre 2018. La Cour constate que les décisions du CSI sont contraignantes, qu'elles font l'objet d'un faible contrôle de la part de l'APD et d'un contrôle juridictionnel mais qu'elles ne sont pas soumises au contrôle parlementaire.

Autorités de contrôle (4/6)

- **Comité de sécurité de l'information**

Compétence du CSI d'accorder des autorisations pour l'utilisation secondaire de données personnelles (2/2)

Les personnes concernées sont donc privées de la garantie d'un contrôle par le Parlement, sans que cela soit imposé par le droit européen. Par ailleurs, l'habilitation critiquée porte sur des éléments essentiels, puisque les législateurs n'ont pas identifié les destinataires de la communication des données concernées. La Cour en conclut que l'habilitation critiquée est inconstitutionnelle. Afin de répondre aux critiques de la Cour constitutionnelle, la loi du 23 novembre 2023 concernant des mesures de police administrative en matière de restrictions de voyage et de formulaire de localisation du passager a été adoptée et modifie diverses dispositions relatives au CSI. Ainsi, il est désormais prévu que la chambre sécurité sociale et santé du comité de sécurité de l'information fera rapport à la Chambre des représentants ainsi qu'à l'Autorité de protection des données dans certains cas et que le ministre compétent pourra exiger du CSI qu'il adapte sa décision si elle n'est pas conforme par exemple aux législations relatives à la vie privée. Ces dispositions sont entrées en vigueur le 6 décembre 2023.

La compétence du CSI vis-à-vis des communautés et des régions

Dans certains cas, les communications de données à caractère personnel par les administrations publiques et les institutions publiques des communautés et des régions sont également soumises à une délibération préalable du CSI lorsque l'administration publique ou l'institution publique en question a adhéré au réseau de sécurité sociale en vertu de l'arrêté royal du 16 janvier 2002. Une exception s'applique à la communication de données à caractère personnel par ce service public ou cette institution publique à un autre organe de la même Communauté ou Région dans la mesure où les parties ne demandent pas expressément l'intervention du CSI.

Autorités de contrôle (5/6)

- **Comité de sécurité de l'information**

Relations entre le CSI et l'ADS

L'ADS souhaite intervenir en qualité de facilitateur vis-à-vis de l'utilisateur des données et du CSI en vue de faciliter l'accès aux données de (soins de) santé :

- **Accompagner l'introduction des demandes de délibération auprès de la Chambre Sécurité sociale et Santé du CSI.** La pratique montre que les demandeurs/utilisateurs de données (instituts de recherche, industrie, prestataires de services professionnels, institutions publiques, etc.) ne fournissent pas toujours au CSI un dossier suffisamment complet, ce qui nécessite des allers-retours répétés entre le CSI et le demandeur. Cette situation nuit au traitement harmonieux des demandes d'accès aux données. L'ADS peut fournir un accompagnement afin de simplifier et d'accélérer ce processus. Ce rôle de facilitateur peut s'inscrire dans le cadre réglementaire et des missions du CSI, l'analyse des demandes et l'octroi des autorisations demeurant une mission centrale du CSI.
- **Couplage / désignation des demandes d'accès convergentes :** Le CSI reçoit régulièrement des demandes d'accès à des données de (soins de) santé qui concernent des ensembles de données convergentes pour des enquêtes de même ordre. Afin de simplifier l'analyse de la demande, l'ADS peut, en prélude à la délibération de la Chambre Sécurité sociale et Santé, circonstancier dans une note explicative adressée au CSI le contenu de la demande, ainsi que sa similitude avec des demandes antérieures traitées par le CSI dans le cadre de délibérations concrètes. Cette analyse préalable de l'ADS peut faciliter l'examen ultérieur du CSI.

Autorités de contrôle (6/6)

- **Vlaamse Toezichtscommissie**

Compétences

Les compétences sont :

- Avis sur toute question concernant le traitement des données personnelles;
- Pouvoirs d'enquête et mesures correctives;
- Avis facultatif sur les projets de protocoles relatifs à la communication électronique de données à caractère personnel par une autorité à une autre autorité ou à une autorité externe.

Relations entre la Vlaamse Toezichtscommissie et l'APD

En tant qu'entité de contrôle, la Vlaamse Toezichtscommissie est chargé de surveiller l'application du RGPD par les autorités/agences flamandes, telles que le Parlement flamand, les organisations de la Communauté flamande ou de la Région flamande, les provinces et les communes et leurs institutions, les associations et les formes de collaboration des provinces et des communes, les CPAS et leurs associations, etc.

La Vlaamse Toezichtscommissie demande à l'APD de déléguer un membre pour assister à toute délibération de la Vlaamse Toezichtscommissie en tant qu'observateur.

L'ADS ne constitue aucunement une autorité de contrôle. L'ADS n'a pas pour objectif de remplacer l'APD ou le CSI ou ni compromettre ses compétences.

Les flux de données et leurs réglementations applicables (1/30)

- **Banque Carrefour de la Sécurité Sociale**

Explication des flux de données

La BCSS a été créée pour veiller à un enregistrement décentralisé et à un échange bien organisé et sécurisé des données entre les ISS. La BCSS dispose à cet égard d'une structure pour organiser un échange automatisé et sécurisé de données à caractère personnel, sans avoir accès aux données elles-mêmes. Ainsi, en principe, chaque ISS doit s'adresser à la BCSS lorsqu'elle a besoin de données qui se trouvent dans d'autres institutions. Si l'institution requérante a effectivement besoin des données pour l'accomplissement de sa mission, la BCSS transmet cette demande aux autres institutions. Ce n'est pas la BCSS qui décide si les données demandées sont indispensables à l'accomplissement de la mission de l'institution. Cette décision appartient au CSI.

Lorsqu'un échange de données intervient avec une instance autre qu'un service public fédéral, un service public de programme ou une institution d'utilité publique fédérale, une délibération préalable de la Chambre Sécurité sociale et Santé du Comité de sécurité de l'information s'impose.

Points d'attention pour l'ADS

La BCSS a un rôle de facilitateur en matière d'accès aux données sociales similaire à celui attribué à l'ADS en matière d'accès aux données de (soins de) santé. Toutefois, les ISS sont tenues de s'adresser à la BCSS lorsqu'elles souhaitent accéder à des données détenues par d'autres institutions. Cette obligation est conforme à celle qui incombe aux détenteurs de données en vertu du Règlement EHDS.

Si l'ADS est confrontée à des demandes d'accès à des données sociales, lorsque celles-ci sont liées à des données de soins de santé, il incombe à l'ADS de sensibiliser l'utilisateur et de lui fournir toute l'assistance nécessaire pour formuler une demande d'accès aux données sociales.

Les flux de données et leurs réglementations applicables (2/30)

- **Institut national d'assurance maladie et invalidité (INAMI) (1/2)**

La base juridique de l'utilisation des données dans le cadre de l'assurance obligatoire des soins médicaux et de l'invalidité est la loi coordonnée du 14 juillet 1994. L'INAMI utilise des données pour remplir ses missions, pour répondre aux questions en tant qu'assuré social ou prestataire de soins de santé et pour rendre opérationnelles les applications web destinées aux prestataires de soins de santé. **L'INAMI ne partage pas de données personnelles, sauf sur une base légale, comme c'est le cas avec les partenaires suivants** : le SPF Finances, 0NEM et les caisses d'assurance maladie.

La **cellule technique** se charge des deux tâches principales suivantes :

- (1) La collecte, le reliage, la validation et l'anonymisation des données relatives aux hôpitaux

Ces données sont mises à la disposition de la cellule technique par le SPF SPSCAE et l'INAMI poursuivant deux objectifs: (1) l'analyse des liens qui existent entre les dépenses de l'assurance soins de santé et la pathologie traitée et (2) l'élaboration de règles de financement, de normes d'accréditation et de critères de qualité dans le cadre d’une politique de santé adéquate. Le SPF SPSCAE, l'INAMI et la BCSS et le KCE utilisent ces données dans le cadre de leurs missions juridiques ou légales. Aucune autorisation n'est requise pour cette mise à disposition et cette utilisation.

- (2) Le transfert de données personnelles à des tiers

Le Roi dispose de quelle manière et à quelles conditions des données anonymes ou des données dans lesquelles la personne morale est ou peut être identifiée, collectées par la cellule technique, peuvent être mises à la disposition de personnes autres que le SPF SPSCAE, l'INAMI et le Centre Fédéral d’Expertise des Soins de Santé, en tenant compte de la nature et de la finalité de la demande de données. Tout transfert de données personnelles depuis la cellule technique dans ce contexte nécessite une autorisation de principe du CSI.

Les flux de données et leurs réglementations applicables (3/30)

- **Institut national d'assurance maladie et invalidité (INAMI) (2/2)**

Explication des flux de données - *Healthdata.be*

Conformément à l'article 22 de la loi coordonnée du 14 juillet 1994, un accord de coopération a été conclu entre l'INAMI et Sciensano. Cet accord concerne la mise en œuvre de la fourniture des services nécessaires à la collecte, à l'hébergement et à la mise à disposition efficaces et sécurisés de données sur la santé et les soins de santé en vue d'accroître les connaissances épidémiologiques, cliniques et autres (dénommé Healthdata.be). Les services développés par Healthdata.be ne sont pas exclusifs aux projets de Sciensano et de l'INAMI dans le cadre de leur accord de coopération. D'autres autorités et institutions fédérales, communautaires et régionales, des institutions scientifiques, des associations professionnelles et d'autres personnes morales de droit privé peuvent utiliser les services de la plate-forme healthdata pour leurs projets scientifiques de soutien à la politique de la santé et des soins de santé (voir art. 4.4. de l'accord de coopération INAMI-Sciensano). Dans ce cas, la procédure telle que stipulée dans l'accord de coopération s'applique.

Les flux de données et leurs réglementations applicables (4/30)

- **Service Public Fédéral Santé Publique, Sécurité de la Chaîne Alimentaire et Environnement (SPF SPSCAE)**

Le SPF SPSCAE collecte et traite des données dans le cadre de ses différentes missions. Le SPF SPSCAE traite des données de santé et des données médicales. L'article 92 de la loi coordonnée sur les hôpitaux et autres établissements de soins constitue la base légale pour les diverses collectes de données au sein des hôpitaux comme **le SMUR, le SMUREG, les statistiques hospitalières annuelles**, etc. Les articles 97 à 101 de la loi coordonnée relative à l'exercice des professions de santé constituent la base légale pour **la banque de données fédérale permanente des professionnels des soins de santé**. Aussi convient-il de souligner que le SPF SPSCAE, l'INAMI et le KCE mettent des données à la disposition de la cellule technique dans le cadre de leurs tâches légales et en vertu de la loi du 29 avril 1996 portant des dispositions sociales.
La Task Force Vaccination est rattachée au SPF SSCE dans le cadre de ses compétences telles que prévues à l'AR du 23 mai 2001 portant création du SPF SSCE. La Taskforce Vaccination collecte et traite des données personnelles pour informer les citoyens et répondre à leurs questions. La Taskforce recueille et traite également des données de manière anonyme à des fins statistiques et qualitatives, dans le but d'améliorer ses services. D'autre part, la Task Force Testing & Tracing intégrée dans l'INAMI est autorisée à établir une stratégie sur les tests et le traçage. Dans le cadre de ses missions, KCE effectue des analyses basées sur des données codées (pseudonymisées). Elle doit donc avoir accès à certaines données personnelles sur la santé des citoyens belges. Pour de nombreuses études, KCE ne collecte pas ces données directement auprès des citoyens, mais y accède principalement par le biais de certains organismes, tels que le SPF SSCE.

- **Service Public fédéral Sécurité Sociale (SPF SS)**

<u>Explication des flux de données</u>

Le SPF SS collecte et traite des données dans le cadre de ses différentes missions. Le SPF SS traite en particulier des données sociales.

Les flux de données et leurs réglementations applicables (5/30)

- **Statbel**

Explication des flux de données

Statbel collecte, produit et diffuse des chiffres tant pertinents que fiables sur l'économie belge, la société et le territoire national. Statbel fournit toute une série de chiffres sur l'économie, la population et la démographie, le marché du travail, la pauvreté, l'agriculture, l'industrie, les services, le marché du logement, le transport et la circulation, l'environnement, etc.

Pour établir ses statistiques, Statbel recourt autant que possible aux bases de données administratives existantes. En effet, Statbel est légalement mandaté pour recevoir des bases de données administratives et pour organiser des enquêtes.

Toutes les informations que Statbel recueille sur les individus sont protégées par le secret statistique. Outre le secret statistique, seuls les travailleurs qui organisent des enquêtes ou qui recoupent les bases de données administratives entre elles ont accès aux données permettant d'identifier une personne (comme le numéro de registre national, le nom, l'adresse). Dans les bases de données de tous les autres travailleurs, les données sont rendues (pseudo)anonymes afin qu'ils ne puissent pas connaître l'identité précise de la personne.

Points d'attention pour l'ADS

Statbel a été inclus dans cette présentation parce que les données gérées et traitées par Statbel dans le cadre de sa mission de collecte, de production et de diffusion de chiffres fiables et pertinents sur l'économie belge, la société et le territoire national, conformément à la loi du 1er juillet 1962 relative à la statistique publique, peuvent être considérées comme des données de (soins de) santé au sens de l'article 2, 3° de la loi sur l'ADS.

Les flux de données et leurs réglementations applicables (6/30)

- **Centre fédéral d'expertise des soins de santé**

Explication des flux de données

En vertu des articles 262 et suivants de la loi-programme du 24 décembre 2002, le KCE traite des données à caractère personnel relatives à la santé des personnes dans le cadre de ses missions légales. La mission du KCE est de réaliser des études scientifiques rigoureuses et objectives, sur lesquelles les décideurs politiques ou les prestataires de soins peuvent fonder leurs décisions en matière de soins de santé et d'assurance maladie. Le KCE est donc censé indiquer la voie à suivre pour trouver les meilleures solutions possibles en vue d'un accès optimal à des soins de santé de qualité.

Dans le cadre de cette mission, le KCE effectue des analyses basées sur des données codées (pseudonymisées). Elle doit donc avoir accès à certaines données personnelles sur la santé des citoyens belges. Pour de nombreuses études, le KCE ne collecte pas ces données directement auprès des citoyens, mais y accède principalement via plusieurs entités déterminées.

Dans certains cas, le KCE a un accès direct aux données pseudonymisées. C'est le cas pour l'échantillon permanent, qui est établi par l'Agence Intermutualiste. Il existe également un accès direct aux données sanitaires relatives aux séjours hospitaliers.

Dans la plupart des cas, le KCE demande l'autorisation du CSI. Ce n'est qu'après l'approbation du CSI que les données seront mises à la disposition du KCE.

Parfois, le KCE collecte des données personnelles directement auprès des citoyens, des professionnels de la santé, des décideurs politiques ou d'autres acteurs du secteur des soins de santé. Cela se fait généralement sous la forme d'enquêtes, d'entretiens ou de groupes de discussion. Ces données sont collectées uniquement sur la base du consentement éclairé de la personne concernée, à qui sont réexpliqués les conditions et modalités du traitement ainsi que ses droits. Ces données ne sont pas transférées à des tiers, sauf lorsque des sous-traitants sont engagés pour des recherches ou une assistance technique. Ils agissent alors au nom et sous la responsabilité du KCE.

Les flux de données et leurs réglementations applicables (7/30)

- **Agence fédérale des médicaments et des produits de santé (AFMPS)**

Explication des flux de données

Des données personnelles peuvent être traitées dans le cadre des missions de l'AFMPS et pour des activités déterminées. En fonction du contexte spécifique, l'AFMPS peut partager des données avec d'autres organismes (gouvernementaux) belges ou internationaux, pour autant que cela soit réglementé dans un cadre légal. Les données personnelles ne seront pas partagées avec d'autres parties.

Les flux de données et leurs réglementations applicables (8/30)

- **Sciensano**

Explication des flux de données

En vertu de l'article 4 de la loi du 25 février 2018, Sciensano assume aux niveaux fédéral, régional et communautaire un large éventail de missions en matière de santé. Il s'agit entre autres choses de rendre des avis aux autorités compétentes en matière de santé, pour la recherche scientifique, l'expertise scientifique, le soutien à la recherche clinique, etc. Sciensano est en outre responsable, dans le respect des lois applicables en la matière, du traitement, en ce compris de la collecte, de la validation, de l'analyse, de la communication et de l'archivage de données à caractère personnel, notamment en matière de santé publique ou de santé et d'autres informations scientifiques relatives à la politique de santé. À cette fin, Sciensano produit des analyses scientifiques quantitatives et qualitatives fondées sur les informations traitées afin de soutenir la politique de santé. Ces missions sont exercées de façon indépendante ou impartiale.

Sciensano peut partager des informations avec certains acteurs.

Comme indiqué précédemment (cf. la rubrique qui traite de l'INAMI), un accord de coopération a été conclu entre l'INAMI et Sciensano. Cet accord concerne la mise en œuvre de la fourniture des services nécessaires à la collecte, à l'hébergement et à la mise à disposition efficaces et sécurisés de données sur la santé et les soins de santé en vue d'accroître les connaissances épidémiologiques, cliniques et autres (dénommé Healthdata.be). Les services développés par Healthdata.be ne sont pas exclusifs aux projets de Sciensano et de l'INAMI dans le cadre de leur accord de coopération. D'autres autorités et institutions fédérales, communautaires et régionales, des institutions scientifiques, des associations professionnelles et d'autres personnes morales de droit privé peuvent utiliser les services de la plate-forme healthdata pour leurs projets scientifiques de soutien à la politique de la santé et des soins de santé (voir art. 4.4. de l'accord de coopération INAMI-Sciensano). Dans ce cas, la procédure telle que stipulée dans l'accord de coopération s'applique(cf. la rubrique sur l'INAMI et la présentation des règlements pertinents).

Les flux de données et leurs réglementations applicables (9/30)

- **La plate-forme eHealth**

Explication des flux de données

La plate-forme eHealth propose un service associé au traitement primaire des données de (soins de) santé des patients.

La plate-forme eHealth n'enregistre pas de données à caractère personnel relatives à la santé. Les données de santé sont conservées auprès des professionnels de santé et dans des bases de données officiellement agréées (CoBRHA, etc.).

Les banques de données relèvent du système de gestion des utilisateurs et des accès que la plate-forme eHealth est tenue de mettre en œuvre.

Les données sont communiquées par voie électronique aux professionnels de santé dans le cadre de la dispensation des soins. Les données peuvent également être communiquées à des instituts de recherche après anonymisation, ou au moins pseudonymisation, dans la mesure où elles sont nécessaires à la recherche scientifique, après délibération de la Chambre Sécurité Sociale et Santé du CSI.

Les flux de données et leurs réglementations applicables (10/30)

- **Registre du Cancer**

Explication des flux de données

Dans le traitement et l'utilisation de ces données d'enregistrement, la Fondation Registre du Cancer veille au respect à la vie privée. C'est la raison pour laquelle elle ne délivre aucune donnée personnelle, sauf en présence d'une base légale ou d'une autorisation du CSI.

- **Association générale de l'industrie pharmaceutique**

Explication des flux de données

L'Association générale de l'industrie pharmaceutique recueille des données dans le cadre de ses activités. Les membres du personnel et les responsables du traitement des données de l'Association générale de l'industrie pharmaceutique ont accès aux données. Ils n'ont accès aux données personnelles que dans la mesure nécessaire à l'exercice de leurs fonctions. Chacun d'entre eux est soumis aux mêmes obligations et a également un strict devoir de confidentialité.

L'Association générale de l'industrie pharmaceutique peut faire appel à des prestataires de services externes ou à des partenaires pour traiter les données personnelles.

Les flux de données et leurs réglementations applicables (11/30)

- **Le secteur académique**

Explication des flux de données

Le secteur académique a besoin d'accéder à certaines données personnelles sur la santé des citoyens belges pour mener des études et des recherches. Pour de nombreuses analyses, le secteur académique ne collecte pas ces données directement auprès des citoyens, mais y accède principalement par l'intermédiaire de certaines instances, conformément aux procédures et aux autorisations nécessaires du CSI.

- **Ordre des pharmaciens**

Explication des flux de données

L'Ordre des pharmaciens recueille des données dans le cadre de ses activités. Ces données proviennent principalement des personnes concernées elles-mêmes, de divers organismes publics et de divers partenaires impliqués. L'Ordre peut partager les données de la personne concernée avec des acteurs déterminés. À l'exception de ces destinataires, l'Ordre traite les données exclusivement pour l'Ordre et pour son propre usage interne. Les données ne seront pas vendues, transférées ou communiquées à des tiers, sauf accord préalable.

Points d'attention pour l'ADS

En principe, l'Ordre traite les données exclusivement pour l'Ordre et pour son propre usage interne. Les données ne seront donc pas vendues, transférées ou communiquées à des tiers, sauf accord préalable. Toutefois, la déclaration de confidentialité de l'Ordre indique que des exceptions sont prévues.

Les flux de données et leurs réglementations applicables (12/30)

- **Ordre des médecins**

Explication des flux de données

L'Ordre est responsable du traitement des données personnelles de tous les médecins qui sont inscrits sur la liste de l'Ordre des médecins et qui y ont été inscrits par le passé. En outre, l'Ordre traite les données personnelles des employés du Conseil national et des Conseils provinciaux, ainsi que, par exemple, des experts externes, des visiteurs, ou les données nécessaires à l'exécution de ses tâches auprès d'organismes externes. Ces données servent à remplir les différentes missions légales de l'Ordre des médecins. En vue de l'accomplissement de ces missions, l'Ordre peut traiter diverses catégories de données personnelles.

En principe, ces données (personnelles) sont communiquées à l'Ordre directement par les personnes concernées, mais dans certains cas, l'Ordre peut également recevoir des données personnelles de la part de tiers. L'Ordre collabore avec des organisations (internationales) à l'étranger. Dans le cadre de cette coopération, des données personnelles peuvent également être communiquées à ces institutions.

En dehors de ces cas de figure, l'Ordre ne louera pas, ne vendra pas ni ne transmettra de données personnelles à des tiers dans un but lucratif. Les données personnelles permettant de remonter à des personnes individuelles ne seront communiquées à des tiers que s'il existe une base ou obligation légale, si c'est nécessaire pour exécuter un accord avec la personne concernée ou si la personne concernée a explicitement consenti au transfert de ses données.

Points d'attention pour l'ADS

La déclaration de respect de la vie privée de l'Ordre précise qu'en principe, l'Ordre ne partage pas les données, sauf s'il existe une base ou obligation légale, si c'est nécessaire pour exécuter un accord avec la personne concernée ou si la personne concernée a explicitement consenti au transfert de ses données.

Les flux de données et leurs réglementations applicables (13/30)

- **Organismes assureurs**

Explication des flux de données

Les organismes assureurs traitent une série de données dans le cadre de leurs missions légales. Ces données proviennent de plusieurs organismes et peuvent être transférées à des acteurs déterminés.

- **Prestataires de soins désignés par les membres du Comité de l'assurance soins de santé de l'Institut national d'assurance maladie-invalidité.**

Explication des flux de données

Les prestataires de soins doivent pouvoir transmettre les données demandées aux chercheurs de manière sûre et efficace. Healthdata.be fournit l'interface technique qui achemine les données du point a au point b de manière cryptée, sécurisée de bout en bout (par cryptage ou chiffrement) et fiable.

Les services développés par Healthdata.be ne sont pas exclusifs aux projets de Sciensano et de l'INAMI dans le cadre de leur accord de coopération. D'autres autorités et institutions fédérales, communautaires et régionales, des institutions scientifiques, des associations professionnelles et d'autres personnes morales de droit privé peuvent utiliser les services de la plate-forme healthdata pour leurs projets scientifiques de soutien à la politique de la santé et des soins de santé. Dans ce cas, la procédure telle que stipulée dans l'accord de coopération s'applique.

Cf. également la rubrique relative aux réseaux locaux ou régionaux (hubs) et aux cellules/coffres-forts.

Les flux de données et leurs réglementations applicables (14/30)

- **Agence inter-mutualiste (IMA)**

Explication des flux de données

IMA rassemble sur une seule plateforme les données des patients provenant des caisses d'assurance maladie et les prépare à l'analyse. Outre les données démographiques et socio-économiques de tous les résidents affiliés au régime d'assurance maladie obligatoire belge, les bases de données de l'IMA contiennent les données de facturation des soins de santé remboursés. Chaque fois qu'un patient a droit à un remboursement, la caisse d'assurance maladie traite et collecte des données telles que le code de nomenclature, la date, le lieu et le coût du service effectué par le prestataire de soins de santé.

Les caisses d'assurance maladie ne transmettent pas les noms et adresses de leurs membres à l'IMA. Le numéro du registre national est codé (pseudonymisé) avant l'envoi des données.

IMA effectue ses propres analyses sur les données, que ce soit ou non à la demande des partenaires légaux. Il réalise également des projets de recherche en collaboration ou à la demande d'agences du gouvernement fédéral, de Régions et de Communautés et en coopération avec des universités.

IMA met ses bases de données à la disposition des chercheurs. Il aide les chercheurs depuis la délibération du CSI jusqu'à la validation et l'interprétation des résultats

Les flux de données et leurs réglementations applicables (15/30)

- **Centres publics d'action sociale (CPAS)**

Explication des flux de données

Le CPAS collecte différentes catégories de données. Le CPAS partage certaines données personnelles avec divers services publics ou institutions privées dans le cadre de l'exécution de ses missions lorsqu'il y est contraint par la loi ou une décision de justice. Le CPAS transfère certaines données personnelles à son sous-traitant dès lors que cela s'avère strictement nécessaire au fonctionnement d'applications ou de systèmes de gestion existants auxquels le CPAS a adhérés.

Si les données personnelles ne sont pas fournies directement par le citoyen, elles proviennent des bases de données publiques auxquelles le CPAS a accès pour l'exécution de ses tâches, par exemple de la Banque Carrefour de la Sécurité Sociale (BCSS).

Les flux de données et leurs réglementations applicables (16/30)

- **Wallonie**

Explication des flux de données

L'Agence pour une Vie de Qualité (AVIQ) est l'agence wallonne chargée des politiques de santé, familiale, des handicapés, du troisième âge et des prestations familiales. L'agence gère les données spécifiques aux compétences de l'AVIQ (allocations familiales, etc.). L'AVIQ traite et stocke différents types de données personnelles relatives à la personne, à la situation familiale, aux données médicales et sanitaires, aux données sociales, aux données financières, aux activités professionnelles, etc.

Seuls les prestataires de soins de santé participant à la continuité des soins aux patients, c'est-à-dire aux activités de diagnostic, de traitement ou de prévention, ont accès aux données des patients. Si les données sont analysées à la demande d'organismes publics ou scientifiques, elles seront anonymisées ou pseudonymisées, et uniquement avec le consentement du conseil d'administration de la FRATEM (qui pilote le Réseau Santé Wallon) et de l'APD. Le principe de départ est que l'accès aux documents d'un patient est interdit, sauf s'il est nécessaire pour atteindre ou soutenir la réalisation de l'une des finalités décrites. Dans ce contexte, les prestataires de soins de santé qui ont accès aux documents doivent encore se limiter aux documents strictement nécessaires à l'exécution de leur propre tâche, et uniquement pour la durée nécessaire à leur exécution. Toutes les personnes qui ont accès aux documents des patients sont tenues au secret professionnel. Aucune donnée, sous quelque forme que ce soit, ne peut être communiquée à des tiers sans le consentement du patient. L'accès aux documents d'un patient doit toujours être justifié par l'intérêt exclusif du patient.

Par ailleurs, le Réseau santé wallon participe à l'échange de données de santé entre systèmes de données de santé connectés via le répertoire de référence de la plateforme eHealth, dont les principes sont définis au niveau fédéral. Le Réseau Santé Wallon applique les principes de "régulation de l'accès" définis à ce niveau.

Les flux de données et leurs réglementations applicables (17/30)

- **Fédération Wallonie-Bruxelles**

Explication des flux de données

La plupart des compétences en matière de santé de la Fédération Wallonie-Bruxelles ont été transférées à la Région wallonne et à la Commission communautaire française. Il convient toutefois de noter que la Commission communautaire commune est devenue l'acteur central bruxellois en la matière suite à la sixième réforme de l'État et suite au protocole d'accord conclu entre le Collège de la Commission communautaire française (COCOF) et le Collège uni de la Commission communautaire commune (CGC) de la Région de Bruxelles-Capitale le 20 novembre 2014 concernant la transition des institutions situées dans la zone bilingue de Bruxelles-Capitale. L'accréditation des prestataires de soins de santé relève de la compétence de la Fédération Wallonie-Bruxelles pour ce qui est des affaires francophones. La Fédération-Wallonie Bruxelles est également responsable à Bruxelles, entre autres, des hôpitaux universitaires francophones et de l'aide à la petite enfance (Office National de la Naissance et de l'Enfance, "ONE"). En vertu de ses compétences, l'ONE traite plusieurs catégories de données.

Nous renvoyons pour le surplus à la section relative à la Wallonie.

Les flux de données et leurs réglementations applicables (18/30)

- **Flandre**

Le Département Zorg soutient et régit toute une palette d'initiatives liées à la santé et aux soins.

Les prestataires de soins et d'assistance peuvent partager électroniquement avec d'autres prestataires de soins et d'assistance les données (personnelles) d'un usager avec lequel ils ont une relation thérapeutique ou de soins. En l'occurrence, il s'agit de données figurant au dossier électronique médical ou de soins qui sont pertinentes pour les soins de leur usager. Les établissements, les prestataires de soins et d'assistance, les mutualités et d'autres acteurs ont un rôle important à jouer par l'intermédiaire de « l'Agence flamande pour la coopération en matière de partage de données entre acteurs des soins (VASGAZ), qui a été créée pour mener le réseau à bien.

Enfin, l'Institut flamand pour la qualité des soins (VIKZ) vise à rendre transparente et à améliorer la qualité des soins et la sécurité des patients dans différents secteurs des soins de santé et des soins résidentiels flamands. Les statuts du VIKZ stipulent en outre que le VIKZ atteint son objectif de qualité des soins et de sécurité des patients, entre autres

« en fournissant *l'information aux, et en passant par la formation, l'accompagnement et le soutien des personnes ou organismes qui développent des instruments de qualité tels que, entre autres, des indicateurs et des méthodes d'audit et en confiant la collecte et le traitement des données de santé sous forme d'indicateurs à un tiers de confiance. Ces données peuvent provenir des différentes sources de données auxquelles les autorités flamandes et fédérales ont accès ou qui sont mises à leur disposition par, entre autres, les différents prestataires de soins de santé, le SPF Santé publique, l'INAMI, la Fondation « Registre du Cancer », l'Institut scientifique de santé publique (WIV) ou l'agence Intermutualiste IMA. Les données collectées par des associations scientifiques ou d'autres institutions peuvent également être traitées par le biais du tiers de confiance. La collecte et le traitement des données s'effectuent conformément aux dispositions légales en matière de protection de la vie privée et des données de santé et aux autorisations accordées à cet égard par le comité sectoriel de la santé.* »

Les flux de données et leurs réglementations applicables (19/30)

- **La Commission communautaire commune**

Explication des flux de données

Iriscare est un organisme d'intérêt public (OIP) bicommunautaire devenu le point de contact privilégié pour les citoyens et les professionnels pour tout ce qui concerne la protection sociale en Région bruxelloise. Iriscare collecte et traite des données à caractère personnel dans le domaine de la santé, de l'assistance aux personnes et des allocations familiales dans la Région bilingue de Bruxelles-Capitale.

Le Réseau Santé Bruxellois est la plate-forme de partage de données médicales créée par l'asbl Abrumet. Le Réseau Santé Bruxellois est un réseau de partage de données médicales électroniques. Il relie tous les hôpitaux bruxellois et belges aux prestataires de soins de santé enregistrés sur le Réseau Santé Bruxellois et permet de collecter les données des patients (résultats d'examens, rapports médicaux, lettres, etc.) partagées par les acteurs des soins de santé. Le projet BruSafe fait partie du hub du Réseau Santé Bruxellois. Ce projet vise à stocker et à partager les données provenant des prestataires de soins de santé. L'architecture de BruSafe coïncide avec celle de son « hub ». Le serveur BruSafe peut être considéré comme une sorte de « fournisseur de données » du hub (comme un hôpital connecté au hub) qui contient les données chargées par les prestataires de soins de santé de première ligne. Le Réseau Santé Bruxellois traite les données nécessaires au bon fonctionnement de la plate-forme, qui servent à valider les demandes des patients et des acteurs des soins de santé.

En ce qui concerne les conditions d'accès par un prestataire de soins, l'objectif est de déterminer si un acteur des soins de santé est autorisé (ou non) à effectuer une opération (par exemple une consultation) sur les données d'un patient donné, en fonction d'un contexte donné (par exemple les prestataires de soins de santé traitants ou le médecin de garde).

Pour obtenir de plus amples informations, nous renvoyons à la rubrique relative aux hubs et aux coffres-forts.

Les flux de données et leurs réglementations applicables (20/30)

- **La Commission communautaire flamande**

Explication des flux de données

La VGC est compétente en matière culturelle, éducative et liées à la personne (bien-être et santé). Les compétences de la VGC s'appliquent aux établissements unicommunautaires néerlandophones. La VGC n'est pas habilitée à agir à l'égard des personnes. Le gouvernement flamand supervise le fonctionnement de la Commission communautaire flamande. **La VGC n'échange donc pas de données sur la santé et les soins aux personnes, sauf exceptions spécifiques.** La VGC transmet les données aux organisateurs des activités. L'organisateur traite les données de manière confidentielle et ne les transmet jamais à des tiers. Dans certains cas, la loi oblige la VGC à transmettre ces informations aux autorités judiciaires.

Les flux de données et leurs réglementations applicables (21/30)

- **la Commission communautaire française**

Explication des flux de données

La COCOF est compétente pour les questions culturelles, éducatives et liées à la personne (bien-être et santé). Les compétences de la COCOF s'appliquent aux établissements unicommunautaires francophones. Il s'agit d'institutions qui appartiennent exclusivement à la communauté francophone en raison de leur organisation (pour les questions liées aux personnes) ou de leurs activités (pour les questions culturelles et l'éducation). La COCOF n'est pas habilitée à agir à l'égard des personnes.

La plupart des compétences en matière de santé exercées auparavant par la Fédération Wallonie-Bruxelles ont été transférées à la Région wallonne et à la Commission communautaire française. La Commission communautaire française agit ainsi de manière totalement autonome dans plusieurs domaines spécifiques et légifère par le biais de décrets.

La Commission communautaire commune est l'acteur central bruxellois en matière de santé.

En ce qui concerne le partage des données, la déclaration de confidentialité de la Commission communautaire française prévoit que la COCOF ne collecte des données personnelles que dans la mesure où cela est nécessaire pour remplir une fonction spécifique. Ces informations ne seront pas utilisées à d'autres fins. Les données personnelles collectées et traitées sont destinées uniquement à la personne responsable du traitement. En aucun cas, elles ne seront transférées à des tiers, sauf en cas d'exceptions légales.

Les flux de données et leurs réglementations applicables (22/30)

- **La communauté germanophone**

Explication des flux de données

La communauté germanophone est compétente en matière culturelle, éducative et liées à la personne (bien-être et santé). L'agence compétente en matière de santé en Communauté germanophone est le « Fachbereich gesundheit und senioren ». Dans le cadre de ses compétences en matière de santé, la Communauté germanophone traite des données à caractère personnel. Le Fachbereich gesundheit und senioren collecte des catégories spécifiques de données. Le Fachbereich gesundheit und senioren partage également certaines données à caractère personnel avec diverses parties dans le cadre de l'exécution de ses missions, lorsqu'il y est contraint par la loi ou par une décision de justice.

Les flux de données et leurs réglementations applicables (23/30)

- **BelRAI**

Explication des flux de données

BelRAI permet une évaluation globale des besoins en soins physiques, cognitifs, psychologiques et sociaux d'une personne. Les prestataires de soins collectent des données de manière standardisée et structurée qui peuvent ensuite être utilisées pour créer un plan de soins de qualité pour toute personne nécessitant des services de soins (complexes). Les données sont enregistrées électroniquement par les prestataires de soins. Une plateforme en ligne BelRAI gratuite est proposée à cet effet.

BelRAI est accessible aux praticiens reconnus d'une profession de santé officielle en Belgique. Un prestataire de soins qui se connecte à la plateforme BelRAI ne peut consulter que les données de ses propres patients. Les institutions et les organisations de soins de santé peuvent également intégrer BelRAI dans leur propre environnement logiciel.

Il convient de noter que BelRAI n'est ni un dossier de soins ni un planificateur de soins. Il reste de la responsabilité des prestataires de soins, dans le cadre de leur autonomie professionnelle, d'évaluer et d'estimer les informations obtenues en vue de la planification des soins et du contrôle de la qualité des soins.

Les échanges de données dont dispose BelRAI ne peuvent avoir lieu que sur la base d'une autorisation du CSI.

Les flux de données et leurs réglementations applicables (24/30)

- **Le Registre central de protection des personnes**

Explication des flux de données

La déclaration de confidentialité du Registre central de protection des personnes - dont la gestion a été confiée au SPF Justice - dispose que le SPF Justice partage électroniquement les données à caractère personnel collectées dans le cadre de ses missions légales. Le partage de ces données se fait après autorisation du CSI. Le SPF veille à ce que seules les données strictement nécessaires au traitement concerné soient collectées. Le SPF collecte et traite des données à caractère personnel pour informer le citoyen, répondre à ses questions, traiter les dossiers qui le concernent. Le SPF collecte et traite également des données de manière anonyme à des fins statistiques et qualitatives, afin d'améliorer ses services et de fournir aux citoyens une réponse dans leur langue.

Les flux de données et leurs réglementations applicables (25/30)

- **Recip-e**

Explication des flux de données

Recip-e est un système qui permet de créer et de délivrer des ordonnances électroniques de soins de santé. Recip-e permet à différents prescripteurs (médecins, dentistes, sages-femmes) d'envoyer des ordonnances par voie électronique et en toute sécurité à un serveur. Là, ils sont cryptés et stockés jusqu'à ce qu'ils soient utilisés par le patient avec un fournisseur de soins de santé (pharmacien). Recip-e traite des données à caractère personnel parce que le citoyen utilise ses services et/ou parce que le citoyen les lui fournit lui-même et que ces données sont absolument nécessaires à la finalité de Recip-e.

Recip-e ne vend ni ne donne les données à des tiers et ne les fournit que si cela est nécessaire pour l'exécution d'un accord ou pour se conformer à une obligation légale. Avec les entreprises qui traitent les données en son nom, Recip-e conclut un accord de traitement pour garantir le même niveau de sécurité et de confidentialité des données. Recip-e reste responsable de ce traitement.

Pour l'application Recip-e, Recip-e est obligé de coopérer avec différentes parties pour assurer la transmission de la prescription médicale. Les services fournis par Recip-e ont été approuvés par le CSI.

Les flux de données et leurs réglementations applicables (26/30)

- **Les réseaux (hubs) et coffres-forts locaux et régionaux (1/3)**

Le Règlement relatif à l'échange de données de santé entre les systèmes de santé connectés via le répertoire des références de la plate-forme eHealth dispose que la mise en œuvre des systèmes d'échange décentralisés est liée à l'introduction du répertoire des références. Partant de ce répertoire, il est possible de savoir où se trouve une donnée de santé relative à un patient. Ce répertoire des références se structure en deux couches :

1) **Une première couche est stockée au niveau de la plate-forme eHealth**. Cette couche, dénommée « metahub », contient uniquement une indication du fait qu'il existe une information au sujet d'un patient :

- dans un hub ; ou
- dans un coffre-fort (dans la mesure où il n'est pas affilié à un hub).

2) **Une seconde couche se situe ensuite au niveau des hubs et des autres systèmes d'échange affiliés (comme des coffres-forts)**. En soutien aux fonctionnalités primaires du système du metahub, une des finalités principales des hubs est donc de tenir à jour un répertoire des références qui indique auprès de quel établissement de soins ou autre réseau d'échange affilié au hub se trouve une donnée de santé relative à un patient.

Le répertoire des références de la plate-forme eHealth est donc finalement constitué du répertoire des références du metahub et de l'ensemble des répertoires des références des hubs et des autres systèmes d'échange affiliés.

Les hubs sont les suivants : Abrumet, Réseau Santé Wallon, Collaboratief Zorgplatform, Vlaams Ziekenhuisnetwerk KU Leuven.

Les organisations de prestataires de soins ou les institutions de soins sont responsables des différents hubs.

Les flux de données et leurs réglementations applicables (27/30)

- **Réseaux locaux ou régionaux (hubs) et coffres-forts (2/3)**

Avec un coffre-fort électronique, tous les professionnels de la santé en dehors des hôpitaux et qui ne disposent pas d'un serveur informatique personnel peuvent également participer à la santé en ligne. Les coffres sont les suivants :

- **Vitalink** : la plateforme de coopération des soins de santé primaires qui est chargée d'organiser le système d'échange Vitalink. Vitalink est un projet flamand pour le partage de données sur les soins et le bien-être, principalement pour la première ligne et le patient, en lien avec la deuxième ligne et les soins résidentiels. Vitalink vise à faciliter la coopération autour d'un partage efficace et sûr des données, et notamment des données personnelles, entre tous les acteurs des soins, en vue d'une prise en charge continue et de qualité des usagers des soins. Ceci est conforme au décret relatif à l'organisation du réseau de partage de données entre les acteurs des soins. Le système Vitalink vise le partage multidisciplinaire de données sur la santé et le bien-être entre tous les acteurs primaires impliqués dans la prise en charge du patient, en mettant en place un "coffre-fort" dans lequel les données nécessaires à cette fin peuvent être stockées. Le système Vitalink permet aux clients de :
  - stocker des données de santé (en communiquant un ensemble de métadonnées telles que le "type" de données de santé) ;
  - mettre à jour ces données de santé ;
  - les données de santé relatives à un patient (en prenant en charge quelques critères de recherche supplémentaires tels que le type de données de santé).
- **BruSafe** : le projet BruSafe fait partie du Réseau Santé Bruxellois, lequel vise à stocker et à partager les données provenant des prestataires de soins de santé. L'architecture de BruSafe coïncide avec celle de son "hub". Le serveur BruSafe peut être considéré comme une sorte de "fournisseur de données" du centre (tel qu'un hôpital connecté au centre) qui contient les données chargées par les prestataires de soins primaires.

Les flux de données et leurs réglementations applicables (28/30)

- **Réseaux locaux ou régionaux (hubs) et coffres-forts (3/3)**
  - **Inter-Med** : le projet Inter-Med fait partie du pôle Réseau Santé Wallon et vise à stocker et à partager les données provenant des prestataires de soins de santé. A l'instar de BruSafe, l'architecture d'Inter-Med coïncide avec l'architecture de son "hub". Le serveur Inter-Med peut également être considéré comme une sorte de "fournisseur de données".

Les flux de données et leurs réglementations applicables (29/30)

- **Vaccinnet**

Vaccinnet est une application utilisée en Flandre pour l'enregistrement des vaccinations. Vaccinnet est gérée par l'autorité flamande. Le Comité interministériel de la Santé publique a décidé d'utiliser cette application pour l'ensemble de la Belgique comme plate-forme d'enregistrement des vaccinations COVID-19.

L'enregistrement des vaccins administrés dans Vaccinnet relève toujours de la responsabilité d'un prestataire de soins. En vue d'un suivi optimal de la politique de vaccination et d'une collecte systématique d'informations, il est donc important d'éviter les doublons d'enregistrements des vaccinations. Vaccinnet est destinée aux prestataires de soins et au personnel des établissements de santé, tels que les cabinets médicaux, les pharmacies, les hôpitaux et les centres de soins résidentiels, pour enregistrer les vaccinations des patients.

Dans le cadre de ses missions, Vaccinnet traite différentes données. Vaccinnet ne transfère pas de données à d'autres parties, sauf s'il existe une base légale pour ce faire. Si Vaccinnet doit faire appel à une autre institution gouvernementale ou à une entreprise externe (par exemple, une entreprise d'informatique ou un bureau d'études) pour exécuter une tâche ou créer un dossier, ils ne peuvent traiter les données que dans le cadre convenu. Vaccinnet n'échange pas de données avec des pays situés en dehors de l'Espace économique européen.

Les flux de données et leurs réglementations applicables (30/30)

- **Loi relative à la publicité de l'administration**

Les administrations fédérales doivent assurer une certaine publicité des documents administratifs en leur possession. Certaines exceptions spécifiques sont prévues. Le citoyen a la possibilité d'exercer ce droit et, en cas de refus de l'administration de lui accorder l'accès, la possibilité de saisir la Commission d'accès aux documents administratifs pour qu'elle statue sur la demande ; elle émettra un avis qui, si les conditions sont réunies, appuiera les démarches entreprises par le citoyen qui n'ont pas encore abouti.

Le droit d'accès aux documents administratifs est souvent appliqué dans le domaine de la santé pour accéder aux données de santé.

Éditeur responsable

Agence des données de (soins de) santé

Avenue Galilée 5 boîte 2, 1210 Saint-Josse-ten-Noode

Auteurs mandatés par l'Agence des données de (soins de) santé

Kathleen De hornois – Deloitte Legal-*Lawyers*

Karolien Maerten – Deloitte Legal-*Lawyers*

Manières de citer

De hornois, K. en Maerten, K. (2023). Analyse juridique du cadre légal applicable aux flux de données de santé, Agence des données de (soins de) santé.

HDA.be