Données de santé :
le coeur battant des soins de demain
Symposium 2025
Mutualités libres

Le traitement de données de santé dans le contexte numérique

Quelles sont les bonnes pratiques et pièges à éviter dans un contexte qui évolue rapidement ?

Alexandra JASPAR
Directrice du Service d'Autorisation et d'Avis

Autorité de protection des données
Gegevensbeschermingsautoriteit

Agenda

- Dossier électronique du patient
- Droits des personnes concernées
- Accès aux données de santé
- Niveau de sécurité adapté au risque
- Acteurs de la gouvernance
- Réutilisation à des fins de recherche

Dossier électronique du patient (DEP)

Soins de santé

services dispensés par un professionnel des soins de santé en vue de déterminer, de conserver, de promouvoir, de restaurer et d'améliorer l'état de santé du patient (> loi qualité, loi droits du patient, EHDS, ...)

Contenu minimal

- **Dossier du patient (DP) :** identification patient et médecin, antécédents, résultats d'examens, rapports, avis, diagnostics, objectifs de santé et déclarations d'expression de la volonté, évolution de l'affection et complications, renvois, notes d'hôpital, identité et portée de la compétence de la personne de confiance, exception thérapeutique, volonté du patient de ne pas savoir (art. 33 de la loi qualité)

- **Dossier électronique du patient (DEP) :** catégories prioritaires de données telles que les données de patient essentielles, les prescriptions et délivrances électroniques, l'imagerie, les résultats d'examen et les lettres de sortie (art. 13 et 14 EHDS + actes d'exécution supplémentaires)

- **BIHR :** (futur) concept d'écosystème numérique afin de faciliter
  - l'implication du citoyen à l'égard de ses propres données de santé (accès/input/suivi)
  - l'accès et l'utilisation pour les praticiens professionnels
  - la réutilisation (pour la recherche et la politique)

→ la relation exacte par rapport à l'ancien D(E)P n'est pas (encore) claire

Dossier électronique du patient (DEP)

Conservation

- **délai :** minimum 30 ans et maximum 50 ans (art. 35 de la loi qualité)
- **décentralisé avec un répertoire des références** (art. 5 de la loi eHealth)
- **stockage et accès électroniques** (exécution par arrêté royal → EHDS)

EHDS

- **format d'échange européen du DEP** → interopérabilité et sécurité (actes d'exécution d'ici fin mars 2027)

Dossier électronique du patient – bonnes pratiques et pièges à éviter

- **Un dossier du patient de qualité (complet et à jour) et conservé en toute sécurité, conformément aux obligations légales en la matière (loi qualité et loi relative aux droits du patient)**

- **Focus sur le format européen pour les dossiers électroniques du patient (à partir de 2027)**

Droits des personnes concernées

RGPD (art. 12 e.s.)

- droit à l'information, droit d'accès/de copie et portabilité
- droit de rectification, d'effacement et de limitation
- droit d'opposition (à l'exception de ce qui est imposé légalement)

Droits des patients (art. 9 de la loi relative aux droits du patient)

- droit à un dossier de patient soigneusement tenu à jour
- droit de faire ajouter des documents (par ex. valeurs, objectifs de vie, déclarations de volonté)
- droit d'accès (incl. les notes personnelles du praticien professionnel - excl. des informations relatives à des 'tiers' - 'indirect' en cas d'exception thérapeutique)
- droit d'obtenir une copie (papier ou électronique)
- accès électronique (→ exécution par AR)

Loi qualité (art. 36 et 40)

- droit de limiter l'accès (consentement) et droit à l'information concernant l'accès

Droits des personnes concernées

EHDS (art. 3 e.s.)

- droit d'accès → via des services d'accès (incl. la possibilité de téléchargement électronique - possibilité de limitation/report → 'en collaboration avec un professionnel de la santé')
- droit pour le patient d'ajouter lui-même des informations
- droit de rectification via une simple demande en ligne
- droit à la portabilité (transfrontalière → format d'échange européen DEP)
- droit de limiter l'accès (règles et garanties fixées par les États membres) et droit à l'information concernant l'accès (qui, quand, quoi au cours des 3 dernières années, notamment via des notifications automatiques)
- droit d'opt-out (règles et garanties fixées par les États membres → par ex. intérêts vitaux)

+ **accès pour les professionnels de la santé → via des services d'accès pour les professionnels de la santé (les États membres peuvent prévoir des garanties supplémentaires)**

Droits des personnes concernées – bonnes pratiques et pièges à éviter

- Fournissez spontanément des informations complètes, compréhensibles et actualisées, adaptées à chaque patient (par ex. en remettant un document lors de l'accueil et via une page web)
- Facilitez l'exercice des droits des personnes concernées : informations sur le point de contact, les procédures, ... et fournissez ensuite en temps utile une réponse claire et complète à la personne concernée
- Accordez une attention particulière à la possibilité pour les patients de limiter l'accès à leurs données de santé et d'obtenir des informations sur l'accès effectif à leur dossier

Accès aux données de santé (art. 36 e.s. de la loi qualité – art. 8 e.s. EHDS) – avis 52/2024

Consentement

- **pour l'accès aux données de santé enregistrées/conservées par un autre professionnel**
- **'tout ou rien' vs 'granulaire'**
  - en ce qui concerne les professionnels (uniquement par le biais d'exclusions)
  - en ce qui concerne le contenu/les documents (non précisé)
- **informé et explicite (verbalement ou par écrit ?)**
- **exception = urgence** (BE : uniquement en cas d'ambiguïté concernant le consentement)

Relation thérapeutique

- **relation entre le professionnel et le patient dans le cadre des soins de santé**
- **exclusion de la médecine de contrôle et d'assurance** (sauf cadre légal spécifique)

Conditions

- **la finalité de l'accès est la prestation de soins de santé dans l'intérêt du patient**
- **l'accès est nécessaire à la continuité et à la qualité des soins de santé**
- **l'accès est limité aux informations pertinentes**

Contrôle des accès journalisés

- **Qui ?**
- **Quand ?**
- **Quoi ?**

Accès aux données de santé – bonnes pratiques et pièges à éviter

- Informez-vous sur la possibilité et les modalités d'autorisation d'accès aux données de santé, ainsi que sur la possibilité d'exclusions (professionnels ou contenu/documents)
- Le consentement est éclairé et explicite
- Organisez un contrôle 'a priori' via une matrice d'accès qui tient compte du consentement, de la qualité (de la personne qui accède aux données) et de la nécessité
- Organisez un contrôle 'a posteriori' via des journaux d'accès (qui, quand, quoi)

Niveau de sécurité adapté au risque

Analyse d'impact relative à la protection des données (AIPD) (art. 35 et 36 du RGPD)

- **identification des risques**
- **en cas de risque résiduel élevé : consultation préalable de l'APD**

Loi-cadre belge sur la protection des données (art. 9)

- **liste des catégories de personnes ayant accès (incl. leur qualité)**
- **liste mise à la disposition de l'APD**
- **obligation de confidentialité**

Protection des données dès la conception et par défaut (art. 25 du RGPD)

- **stockage décentralisé – répertoire des références** (indication des données de quel patient chez quel acteur des soins de santé) (art. 5 de la loi eHealth) (→ avis n° 127/2023)
- **mesures techniques/technologies renforçant la confidentialité telles que le chiffrement (homomorphe) et les audits système périodiques**
- **gestion qualitative des utilisateurs et des accès avec identification et authentification correctes et journalisation**
  - recommandation n° 01/2008
  - haut niveau de fiabilité de l'identification et de l'authentification (eIDAS) → eID et itsme

Niveau de sécurité adapté au risque – bonnes pratiques et pièges à éviter

- **Vérifiez si une AIPD (et une consultation de l'APD) est (sont) nécessaire(s) et pensez aux technologies renforçant la confidentialité**
- **Tenez à la disposition de l'APD un registre des personnes autorisées à accéder aux données**
- **Mettez en place une gestion qualitative des utilisateurs et des accès avec identification et authentification correctes et journalisation**
- **Prévoyez la formation et la sensibilisation nécessaires en matière de protection des données et de la politique en la matière**

→ Décision quant au fond 166/2024 de la ChC du 17 décembre 2024 concernant les mesures de sécurité (insuffisantes) prises par un hôpital

Gouvernance – acteurs

- **Droits du patient** **(art. 16 de la loi relative aux droits du patient)**
  - **Service de médiation** (information – recommandations – traitement des plaintes)
  - **Commission fédérale 'Droits du patient'** (conseil et évaluation)

- **Loi qualité**
  - **Commission fédérale de contrôle** (contrôle de tous les aspects de la qualité de la pratique) (→ avis n° 109/2025)

- **Loi BCSS et loi eHealth**
  - **Plateforme eHealth** (art. 4 et 5 de la loi eHealth) (→ avis n° 127/2023)
    - échange d'informations par voie électronique dans le domaine des soins de santé
    - services de base tels que le cryptage, la datation électronique, la pseudonymisation/anonymisation, le répertoire des références
  - **Chambre Sécurité sociale & Santé du CSI**
    - bonnes pratiques (notamment en matière de protection des données)
    - délibérations à portée limitée et technique (art. 46 de la loi BCSS et art. 11 de la loi eHealth) (→ avis n° 268/2022)

Gouvernance – acteurs

- **ADS** > faciliter/conseiller en matière de disponibilité (via le catalogue de métadonnées) et de réutilisation des données de santé (→ avis n° 234/2022)
- **RGPD**
  - **> Autorité de protection des données**
    - **Service d'Autorisation et d'Avis** (avis sur les projets normatifs)
    - **Secrétariat Général** (avis en matière d'AIPD à risque résiduel élevé - fuites de données)
    - **Service de Première Ligne** (sensibilisation et médiation) **et Chambre Contentieuse** (règlement des litiges)
- **EHDS**
  - **autorités chargées de la santé numérique > exécution et application au niveau national** (information – surveillance – traitement des plaintes) **– coopération avec d'autres autorités** (dont l'APD)
  - **points de contact nationaux pour la santé numérique reliés à MyHealth@EU :** plateforme d'échange transfrontalière à créer par la CE (→ actes d'exécution)

→ **pour l'instant, on ne sait pas encore quelles autorités belges assumeront les rôles décrits dans l'EHDS** (→ notification à la CE avant fin mars 2027)

Gouvernance – acteurs – bonnes pratiques et pièges à éviter

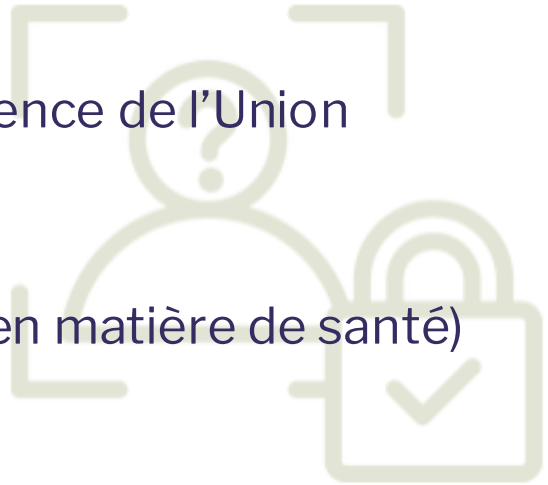
- **Information des patients concernant :**
  - l'existence des divers acteurs et leurs missions respectives
  - Les points de contact et les procédures à suivre

Réutilisation à des fins de recherche

- **Articles 5.1.b) et 89, paragraphe 1 du RGPD**
  - le traitement ultérieur à des fins de recherche n'est en principe pas incompatible
  - garanties appropriées → minimisation des données → cascade : anonymes – pseudonymisées – non pseudonymisées
- **Loi-cadre belge sur la protection des données – Titre 4**
  - applicable en cas de limitation des droits des personnes concernées
  - contrat entre le responsable du traitement initial et le responsable du traitement ultérieur
  - tiers de confiance pour l'anonymisation/la pseudonymisation en cas de couplage de données
- **Loi santé du 13/12/2006 (art. 42) et loi eHealth (art. 11)**
  - autorisation de principe de la Chambre SS&S du CSI pour la communication de données de santé (via la plateforme eHealth ou non) (→ avis n° 268/2022)
- **Lignes directrices européennes en matière de recherche scientifique (dans le domaine de la santé) (début prévu début 2026)**
- **EHDS**
  - faciliter et maximiser la réutilisation de données de santé à des fins de recherche, de politique et de statistiques
  - instances chargées de l'accès : octroi/refus d'autorisations d'utilisation et d'accès
  - mise à disposition obligatoire sauf en cas d'opt-out (sauf exclusion en droit national pour des raisons d'intérêt public)
  - catalogue public d'ensembles de données
  - également transfrontalier → HealthData@EU via des points de contact nationaux

Réutilisation à des fins de recherche – bonnes pratiques et pièges à éviter

- **Anonymisation et pseudonymisation de qualité**
  - Pseudonymisation ≠ anonymisation
  - Attention au risque de réidentification par le biais d'un processus d'individualisation, de corrélation ou d'inférence
- **Techniques d'anonymisation transparentes :** avis 05/2014 Groupe de travail "Article 29"
- **Bonnes pratiques en matière de pseudonymisation :** rapports de l'Agence de l'Union européenne pour la cybersécurité (ENISA)
- **EDPB :** lignes directrices européennes pour la recherche scientifique (en matière de santé)



Merci pour votre attention !

Alexandra.jaspar@apd-gba.be

Rue de la presse 35, 1000 Bruxelles
Drukpersstraat 35, 1000 Brussel

T +32 (0)2 274 48 00
contact@apd-gba.be

Autorité de protection des données
Gegevensbeschermingsautoriteit
APD – GBA