Analyse d’impact relative à la protection des données: défis de mise en place

AGENCE eSanté LUXEMBOURG | Agence nationale des informations partagées dans le domaine de la santé

Nouveau règlement sur la protection des données
Conférence CNPD-SMC 11/10/2016

my DSP

Agenda

1. Agence eSanté
2. Définition Analyse impact protection données
3. Analyse d'impact – retour d'expérience
4. Les défis à venir, vers le GDPR

Agence eSanté – Présentation

L'Agence eSanté est un Groupement d'Intérêt Économique, **créé par la loi du 17 décembre 2010 et opérationnel depuis l'été 2012**.

Objectifs (art. 60ter and 60quater Code de la Sécurité Sociale)

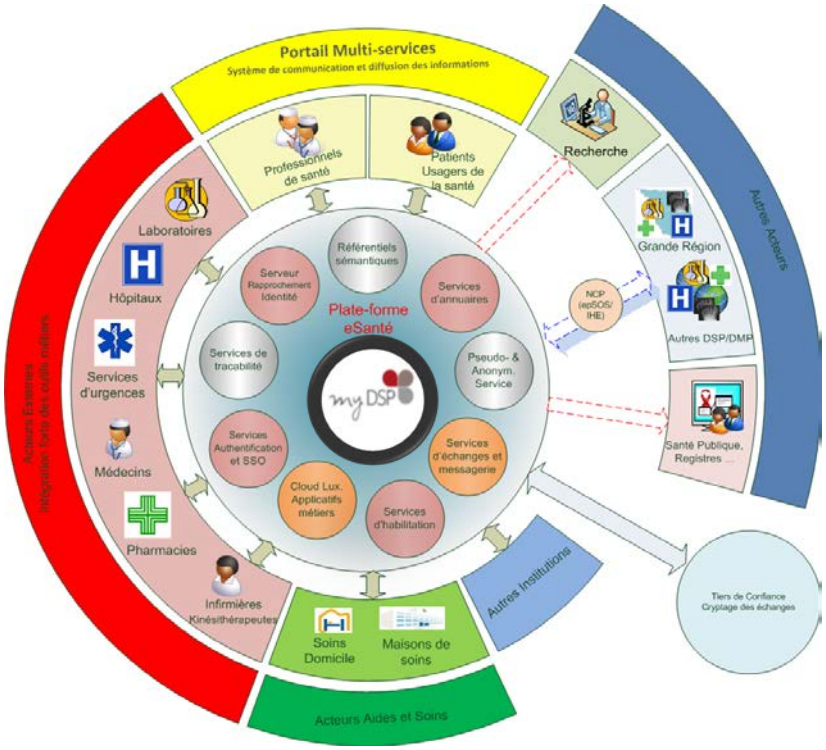
- Faciliter une communication fluide et continue entre les professionnels de santé
  => Continuité des soins
- Améliorer la transmission des informations de santé autour du patient et du médecin référent
  => Coordination des soins

L'Agence eSanté GIE est gouvernée par un Conseil de Gérance dont les membres sont des représentants des institutions et des professionnels de la Santé du Grand-Duché.

Agence eSanté – Présentation

La **Plateforme Nationale eSanté**:

- C'est une plateforme d'**échange et de partage de données de santé dématérialisées** (électroniques).
- Elle comprend services opérationnels aujourd'hui :
  - ❖Des services d'**annuaires** (des patients et des professionnels de santé);
  - ❖Des services de **sécurité**, de **traçabilité** et d'**authentification;**
  - ❖Une **messagerie sécurisée de santé** (utilisation généralisée par SHD pour leurs soignants);
  - ❖Des services santé spécialisés: Dispositif **Médecin Référent** (ouverture 1er juillet 2016), **Dossier Patient Informatisé** pour établissement de santé (IdeoMed), **serveur de terminologies;**
  - ❖Le **Dossier de Soins Partagé** (DSP) – phase pilote lancée en juin 2015: création de DSP pour les patients, connexion par les prestataires de soins (RGD en cours élaboration)



Le Dossier de Soins Partagé (DSP)

Le Dossier de Soins Partagé est :

- dossier de santé électronique **gratuit**, **personnel** et **sécurisé**, qui regroupe les **données de santé essentielles** pour le suivi du patient ;
  - ❖Objectif : Favoriser la continuité, la coordination et la sécurité des soins au patient, et une meilleure utilisation des données de santé
- **Accessibles au patient et aux professionnels de santé** intervenant dans la prise en charge du patient (**lien thérapeutique**)
  - ❖Pour le patient : utilisation du portail eSanté + Carte LuxTrust ou OTP
  - ❖Pour le professionnel de santé

Droits du patient sur le DSP :

- ❖ consultation des données de santé déposées par les professionnels de santé
- ❖ gestion des accès au DSP et définition du niveau de confidentialité des documents
- ❖ dépôt de document dans la zone «Expression personnelle »
- ❖ fermeture et réouverture du DSP
- ❖ consultation des traces d'accès (qui, quand, pour quelle raison)

Agenda

1. Agence eSanté
2. Définition Analyse impact protection données
3. Analyse d'impact – retour d'expérience
4. Les défis à venir, vers le GDPR

Définition analyse impact protection des données

Identification des risques pour les droits et libertés des personnes physiques (considérant 75)

Nature, finalités et contexte du traitement

- profilage, décision automatisée
- évaluation, prédiction analyse comportement

Degré de gravité

- Données sensibles
- Volume de données, nombre de personnes concernées
- Personnes vulnérables (ex. enfants)
- Dommages physiques, matériels ou moral
  - atteinte à l'intégrité physique
  - vol, usurpation d'identité, perte financière
  - discrimination, atteinte à la réputation, perte de contrôle

Degré de probabilité

Définition analyse impact protection des données

Art. 35 (7) RGPD – Contenu a minima du DPIA

Description du traitement : finalités, processus, intérêt légitime (ou opérations de traitement similaires qui présentent des risques élevés similaires)

Evaluation de la nécessité et de la proportionnalité

Evaluation objective des risques pour les droits et libertés des personnes concernées compte tenu de la nature, de la portée, du contexte et des finalités du traitement

Mesures et mécanismes

- traitant les risques,
- assurant la sécurité et protection des données
- apportant la preuve du respect du RGPD

Définition analyse impact protection des données

Application de l'approche basée sur le risque

Limiter ou éviter le potentiel préjudice pour les personnes et garantir leurs droits

Déterminer le niveau des obligations et assurer la conformité

Art.24 (1) Responsabilité du responsable de traitement

Mise en œuvre et contrôle des mesures techniques et organisationnelles appropriées au regard des risques pour s'assurer du respect du RGPD et être en mesure de démontrer son respect

Art. 33 et 34 Notification et communication de violation de données à caractère personnel

Contenu de la notification (personnes impactées, conséquences probables), bénéfice de l'exception (violation n'engendre pas un risque pour les personnes)

Communication auprès des personnes en présence de violation engendrant un risque élevé

Art 83 (2) Sanction administrative

Critères de détermination de la sanction (ex: nature et gravité de la violation, nombre de personnes impactées, dommages, mesures en place pour la sécurité et limiter le dommage)

Définition analyse impact protection des données

Travaux du G29

Plan d'action pour l'implémentation du RGPD
http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

⇒ Lignes directrices concernant le DPIA
publication estimée fin 2016 – début 2017

- Critère d'identification des traitements à risque élevé
- Principes clés de conduite d'un DPIA

Travaux existants concernant le DPIA

CNIL : PIA, la méthode : Comment mener une étude d'impact sur la vie privée
https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf

ICO : Conducting privacy impact assessments code of practice
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

CIPL : Privacy Risk Framework and the Risk-based Approach to Privacy
https://www.informationpolicycentre.com/cipl-white-papers.html

AGENDA

1. Agence eSanté
2. Définition Analyse impact protection données
3. Analyse d'impact – retour d'expérience
4. Les défis à venir, vers le GDPR

Analyse impact – retour d'expérience

Exigence légale : **Haut niveau de sécurité et de confiance** auprès des patients, professionnels de santé et autres acteurs du secteur (art. 60quater CSS)

Réalisation phase pilote pour évaluer le dispositif avant entrée en vigueur RGD

Février **2014** : Demande **PIA** pour obtenir tous les éléments lui permettant de donner son **avis quant à l'adéquation des dispositifs opérationnels**

Avril **2015 :** accord pour le déploiement du DSP en phase pilote

Questionnaire "Evaluation sécurité et des risques sur la vie privée"

⇒ démonstration de la conformité du traitement (mesures, règles internes, documentation)
⇒ base méthode CNIL adaptée à la législation applicable au secteur de la santé du Luxembourg

<u>Exigences générales – management de la protection des données</u>
Gouvernance, gestion des risques sur la vie privée, Privacy by design

<u>Exigences spécifiques relatives au respect des droits - conformité aux principes</u>
Processus de collecte des données, informations des patients, exercice de leurs droits

<u>Exigences spécifiques relatives à la protection des données - mesures pour la sécurité</u>
Traçabilité des activités, Contrôle des accès, Chiffrement des données, Gestion des vulnérabilités

Analyse impact – retour d'expérience

Démarche suivie - Appui sur le SMSI mis en œuvre par l'Agence eSanté

Action conjointe RSSI et DPO

Vision globale et transversale

Appui sur les actions et initiatives existantes (internes et externes)

Challenges

Cohérence, compréhension et objectif – analyse « hors des murs » de l'agence

Estimation des ressources nécessaires et charge de travail

Identification et niveau d'implication des acteurs pertinents

Absence base de connaissance (échelles, impacts)

Efficience (valeur ajoutée des actions dans le temps)

Analyse impact – retour d'expérience

Analyse d'impact sur les personnes via l'analyse de risque sur la sécurité de l'information

Appui sur la méthodologie CNIL "Gérer les risques sur les libertés et la vie privée" basée sur la méthode de gestion des risques EBIOS conforme aux normes ISO27001, ISO27005…

<u>Définition du contexte – périmètre de l'étude</u>

- description traitement – processus (schéma)
- identification supports, catégorie de données
- mesures juridique et respect droits de la personne concernée

<u>Identification du Risque sur la personne concernée</u>

Accès illégitimes aux données

Modifications non désirées

Disparition

Source humaine ou non-humaine

Source interne ou externe

Accidentelle ou délibérée

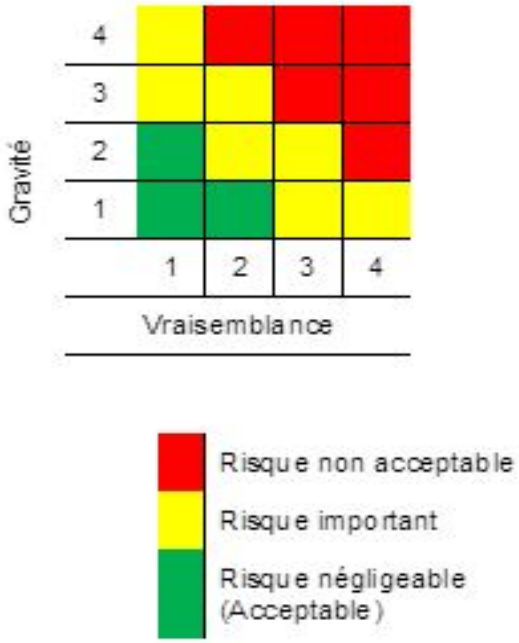
Analyse impact – retour d'expérience

Echelle de gravité

Impacts sur la personne (P)			Exemples
0	Pas d'impact		
1	Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	Corporel : maux de tête Matériel : perte de temps pour réitérer des démarches, réception spams Moral : agacement, sentiment intrusion commerciale
2	Limité	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	Corporel : affection mineure (maladie bénigne) Matériel : frais supplémentaires, promotion professionnelle manquée Moral : peur, stress, intimidation sur réseau sociaux
3	Important	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés	Corporel : aggravation de l'état de santé, atteinte intégrité temporaire Matériel : interdit bancaire, perte de logement, perte emploi, escroquerie Moral : victime de chantage, harcèlement, assignation en justice
4	Maximal	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	Corporel : décès, affection permanente, altération définitive intégrité physique Matériel : impossibilité de travailler, perte accès eau, péril financier Moral : enlèvement, perte lien familial

Analyse impact – retour d'expérience

Cartographie des risques

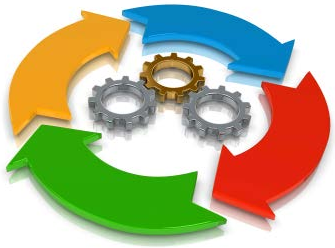


Identification des mesures de sécurité pour traiter les risques

- Mesures techniques et organisationnelles
- Intégration des aspects protection des données et vie privée
- Action demandée auprès des sous-traitants

Identification et acceptation des risques résiduels

⇒ Justification : état des connaissances, nature, coûts, portée



Réévaluation des risques

- Revue périodique à minima
- Survenance d'un incident (interne et apprentissage incident externe)
- Modification traitements et mesures de sécurité (evolution technologique, projets, …)

Agenda

1. Agence eSanté
2. Définition Analyse impact protection données
3. Analyse d'impact – retour d'expérience
4. Les défis à venir, vers le GDPR

Les défis à venir, vers le RGPD

… ce que l'on retient

Une analyse « allégée » du traitement doit être réalisée pour déterminer la nécessité du DPIA, et permettre le respect du GDPR (registre, démonstration de la conformité)

DPIA est une analyse spécifique, mais liée aux analyses de risque existantes en interne

Cela ne peut être un simple questionnaire à compléter, les méthodologies des métiers et les livrables correspondants doivent être associés

Le DPIA doit suivre une démarche itérative, pour être intégré au plus tôt dans les projets et « accompagner » le traitement dans le temps

Le DPIA n'est pas la tâche exclusive du DPO, il doit être réalisée par une personne ayant une vue globale et transversale et dont les résultats et risques doivent être acceptés par la direction

Les défis à venir, vers le GDPR

… ce que l'on attend

Précision et définition des critères requérant la réalisation obligatoire d'un DPIA

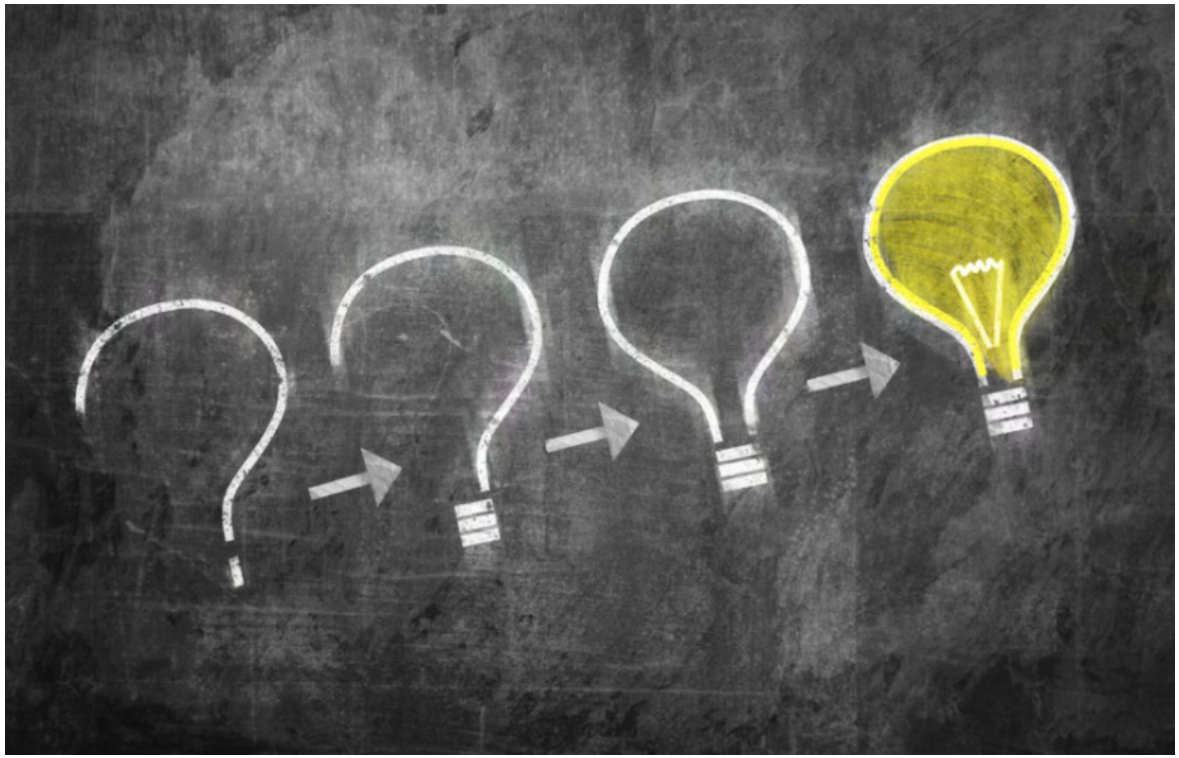
Identification de la méthodologie à suivre et/ou des méthodologies équivalentes acceptées

Précisions des bases de connaissances concernant les risques sur les personnes et des échelles

Détermination de la forme du DPIA et de son contenu en pratique attendu

Recommandations, lignes de conduite et bonnes pratiques (périodicité, rôle et responsabilité)

Questions



Violaine Langlet, CIPM
Chargé de protection des données - Juriste

+352 2712 5018 32
violaine.langlet@agence-esante.lu

G.I.E. Agence eSanté Luxembourg
Agence nationale des informations partagées dans le domaine de la santé

Bureaux : 125, route d'Esch L-1471 Luxembourg
Siège social : Villa Louvigny – Allée Marconi L-2120 Luxembourg
RC Luxembourg C-69

AGENCE eSanté LUXEMBOURG | Agence nationale des informations partagées dans le domaine de la santé