## Grille d’étude des risques



Méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement exprès de la personne concernée Afin de cadrer la démarche de gestion des risques présentés par le traitement et de justifier de sa mise en œuvre, le responsable de traitement peut renseigner les éléments ci-dessous et les conserver avec la documentation afférente au traitement.

|  |  |
| --- | --- |
| Description du traitement : |  |
| **Finalités du traitement :** |  |
| **Enjeux du traitement :** |  |
| **Responsable du traitement :** |  |
| **Sous-traitants :** |  |

|  |
| --- |
| Schéma fonctionnel du traitementdétaillant les flux de données personnelles et leurs supports |
|  |

**NB** : ce schéma doit s’étendre de la collecte jusqu’à la destruction des données.

|  |
| --- |
| Mesures de sécurité mises en œuvre |
| **Catégories de mesures sur les données du traitement[[1]](#footnote-1)** | **Description des mesures mises en œuvre** |
|  |  |
|  |  |
| **Catégories de mesures générales sur le système d’information[[2]](#footnote-2)** | **Description des mesures mises en œuvre** |
|  |  |
|  |  |
|  |  |
| **Catégories de mesures organisationnelles[[3]](#footnote-3)** | **Description des mesures mises en œuvre** |
|  |  |
|  |  |
|  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Violations potentielles des données du traitement | Impacts potentiels sur la vie privée des personnes concernées | Gravité[[4]](#footnote-4) | Menaces rendant possibles les violations de données | Vraisemblance[[5]](#footnote-5) | Justification |
| **Accès illégitime aux données** |  |  |  |  |  |
| **Modification non désirée des données** |  |  |  |  |  |
| **Disparition des données** |  |  |  |  |  |

**NB** : la gravité des impacts et la vraisemblance des menaces tient compte des mesures de sécurité mises en œuvre. On peut se référer au Guide de la CNIL : « Étude d'impact sur la vie privée », [PIA, l’outillage](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-PIA-2-Outillage.pdf), chapitres 3.2 et 3.3

1. Chiffrement, anonymisation, sécurité des documents papier, … [↑](#footnote-ref-1)
2. Cloisonnement du traitement, moyens d’authentification, profils utilisateurs, journalisation, mises à jour et correctifs, antivirus, équipements mobiles, sauvegarde, maintenance, sécurité réseau, contrôle d’accès physique, sécurité physique, … [↑](#footnote-ref-2)
3. Politique de sécurité, gestion des risques et des incidents, gestion des personnels, relation avec les tiers, … [↑](#footnote-ref-3)
4. Échelle proposée : 1. Négligeable, 2. Limitée, 3. Importante, 4. Maximale [↑](#footnote-ref-4)
5. Idem [↑](#footnote-ref-5)