



Alexis Astruc<sup>1,2,3</sup>, Adeline Jouannin<sup>4,5,6</sup>, Erik Lootvoet<sup>1</sup>, Timothée Bonnet<sup>7</sup>, Frederic Chevallier<sup>1,8</sup>

- 1.. Université Sorbonne Paris Nord, Département universitaire de Médecine générale, DUMG, F-93000 Bobigny
- 2.. Centre de santé Ellasanté, F-75008, Paris
3. Maison de santé Orly Santé, F-94310, Orly
4. Département de médecine générale, Université de Rennes, F-35000 Rennes.
5. Centre d'investigation clinique de Rennes (CIC Inserm 1414), Université de Rennes, CHU Rennes, Inserm, F-35000 Rennes.
- 6.. Centre de recherche des Cordeliers (UMRS1138), INSERM, Sorbonne Université, USPC, Université Paris-Descartes, Université Paris-Diderot, équipe ETREs, F-75006 Paris.
7. Université Sorbonne Paris Nord, Service des archives, F-93430 Villetaneuse
8. MUSSP, 14 rue de la république, 95120 Ermont

alexis.astruc@yahoo.fr

exercer 2021 ; 172:178-84.

## Les données à caractère personnel : quelles formalités réglementaires pour les travaux de recherche en médecine générale ?

Personal data: what are the regulatory requirements for research work in general medicine?

### Annexe 6 - L'analyse d'impact relative à la protection des données (AIPD)

#### L'AIPD contient 4 parties

- Une première partie de contexte décrivant le traitement, les finalités, les typologies de données traitées, les processus (cycle de vie des données), etc.
- La deuxième partie porte sur l'évaluation de l'opportunité de mener le traitement en s'attardant sur la légitimité du traitement, la licéité, la minimisation, la durée de conservation, etc.
- La troisième partie concerne l'évaluation des risques pour les droits et libertés des personnes concernées, et les mesures techniques (chiffrement, pseudonymisation, anonymisation) (Cf. Annexe 3) et organisationnelles (mise en place de contrôles pour l'accès aux données, politique de sécurité des systèmes d'information, etc.) prises par l'organisme afin de faire face à ces risques, qui peuvent avoir des origines internes ou externes diverses (accès illégitime, modification non désirée, disparition, etc.).
- Enfin, la dernière partie fait la synthèse de l'ensemble des éléments précités en

établissant une cartographie des risques et un plan d'action et permettant ainsi une validation par le DPO et le responsable de traitement de l'étude d'impact.

- En pratique, trois scénarios à envisager : accès illégitime aux données / modification non désirée des données / disparition des données. Sous trois angles : impacts potentiels sur la vie privée des gens, gravité, vraisemblance.

#### L'outil PIA de la CNIL

Pour accompagner les responsables de traitement, la CNIL a développé un logiciel à code source ouvert, intitulé PIA, qui facilite la conduite des AIPD. Ce logiciel est disponible en ligne sur le site de la CNIL. Son utilisation nécessite de suivre les questions posées, et d'exporter le résultat pour validation par le DPO.