Le principe d'*accountability* et ses conséquences en matière de santé

En matière de protection des données à caractère personnel, le **principe de transparence** implique, vis-à-vis des autorités, la mise en œuvre de **formalités préalables** par le responsable de traitement.

Selon les règlementations française et européenne actuellement en vigueur, les données de santé sont des **données sensibles**, et leur traitement est par principe **interdit**. Lorsqu'ils sont légalement autorisés, les traitements de données sensibles pourront être licitement mis en œuvre après accomplissement des formalités légales obligatoires.

En matière de santé, **la formalité à réaliser dépendra de plusieurs critères** (finalité du traitement, nature des données, identité du responsable de traitement, etc). Il pourra s'agir d'une **demande d'autorisation** auprès de la CNIL pour les traitements les plus sensibles, ou d'une simple **déclaration à la CNIL** pour les traitements les plus courants. Dans certains cas, des outils peuvent être utilisés pour simplifier encore ces formalités :

- ⇨ **Les méthodologies de référence** simplifient la déclaration du traitement des données à la CNIL puisque le responsable de traitement n'aura plus qu'à s'assurer qu'il est en accord avec ladite méthodologie et en apporter la preuve en cas d'inspection de la CNIL.
- ⇨ **L'Autorisation unique** est un moyen par lequel la CNIL autorise, par une décision unique, tous les traitements ayant une même finalité et des catégories de données et de destinataires identiques.
- ⇨ **Les normes simplifiées**, publiées par la CNIL, visent à simplifier l'obligation de déclaration pour les catégories de traitements de données les plus courantes.

Illustrations :

Procédures simplifiées	Déclaration	Autorisation
Normes simplifiées n°50 pour la gestion des cabinets médicaux et paramédicaux	Fichiers de gestion administrative et médicale	Les traitements justifiés par un intérêt public comportant des données de santé
Autorisation unique pour les traitements relatifs à la pharmacovigilance des médicaments		Les traitements de données sensibles qui recourent, à bref délai, à une anonymisation
Méthodologie de référence pour les traitements relatifs aux recherches biomédicales		Les fichiers mis en œuvre à des fins de recherche médicale

Quel avenir pour les formalités françaises en matière de données de santé ?

Le Règlement Européen change la donne en consacrant le **principe d'*accountability*** (art. 24). Dans une optique de **responsabilisation des acteurs**, le mécanisme actuel de formalités préalables et de contrôle *a priori* des autorités de contrôle fera place à un **mécanisme d'autocontrôle** des responsables de traitement doublé d'un **contrôle a posteriori des autorités**.

L'*Accountability* impose en effet au responsable de traitement :

- ⇨ non seulement de mettre en œuvre les mesures et processus appropriés pour garantir le respect de la règlementation applicable en matière de données personnelles,
- ⇨ mais surtout de **tracer et documenter ces mesures et processus**, afin d'être à même de **démontrer cette conformité aux autorités** en cas de contrôle postérieur à la mise en œuvre du traitement.

En pratique, la mise en œuvre du principe d'accountability se traduit notamment par la mise en place des **outils de conformité** suivants :

- la tenue d'une registre des traitements mis en œuvre (art. 30.) ;
- la réalisation d'un audit de conformité et sa mise à jour ;
- la désignation d'un délégué à la protection des données (DPO) – parfois obligatoire - (art.37) ;
- l'adoption de l'approche *Privacy By Design* et de *Privacy by Default* (art.25);

- la notification des failles de sécurité (art. 33 et 34) ;
- la réalisation d'une étude d'impact sur la vie privée (EVIP) des traitements envisagés (art. 35).

La principale conséquence du principe d'*accountability* est la **suppression des obligations déclaratives** dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.

*Le Règlement européen prévoit cependant que « **Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé** » (article 9.4).*

En matière de santé, le régime français actuel d'autorisation pour certains traitements pourrait donc être maintenue par le droit national.

Pour aller plus loin : l'étude d'impact sur la vie privée (EIVP)

Pour justifier sa démarche de conformité en application du principe d'*accountability*, le responsable de traitement qui souhaite mettre en œuvre un nouveau traitement pourra réaliser une **auto-évaluation des risques** que présente son projet sur la vie privée des individus.

Cette **étude d'impact** devra même être **obligatoirement** réalisée **préalablement** à la mise en œuvre d'un traitement présentant un **risque élevé** pour les droits des individus (article 35 du Règlement). Sont notamment des traitements à risque au sens du Règlement (outre ceux qui seront identifiés comme tels par les autorités de contrôle) :

- ✓ Les traitements impliquant un profilage des individus sur la base desquels des décisions ou mesures sont prises ;
- ✓ Les traitements de surveillance à grande échelle ;
- ✓ **Le traitement « à grande échelle » (*i.e* massif) de données sensibles**

*Le Règlement prévoit que le traitement ne devrait pas être considéré comme étant à grande échelle s'il concerne les **données à caractère personnel de patients, par un médecin ou un autre professionnel de la santé. L'analyse d'impact ne devrait alors pas être obligatoire** (considérant 91).*

L'EIVP permettra d'évaluer la probabilité et la gravité du risque crée par le traitement, et présentera les mesures et garanties envisagées pour atténuer ce risque et démontrer le respect de la règlementation.

Et après ?

- ⇨ Lorsque l'EIVP indique que le traitement présenterait un risque élevé faute de mesures prises pour l'atténuer, le responsable de traitement devra **consulter l'autorité de contrôle préalablement** à la mise en œuvre du traitement (article 36).
- ⇨ Lorsque l'autorité de contrôle estime que le traitement envisagé violerait le règlement ou pourrait présenter un risque insuffisamment atténué, elle fournira un **avis écrit au responsable du traitement et pourra mettre en œuvre ses pouvoirs coercitifs**.

Une **marge de manœuvre** est laissée aux Etats membres pour exiger que le responsable de traitement consulte et obtienne l'autorisation de l'autorité de contrôle préalablement à la mise en œuvre d'un traitement effectué dans le cadre d'une mission d'intérêt public, de la protection sociale ou de la santé publique. L**e droit national pourra ainsi maintenir un régime de formalités en matière de santé publique**.