# NEWSLETTER E-SANTE

NUMÉRO 8 ● 2023

## ÉQUIPE


**Alexandre FIEVEE**
Avocat associé

**Alice ROBERT**
Avocat senior


## SOMMAIRE

# SANCTION D'UN LABORATOIRE D'ANALYSES MEDICALES

*En sanctionnant un laboratoire d'analyses médicales, l'autorité de contrôle belge est venue clarifier ou rappeler certains principes du RGPD.*

Après avoir réalisé une analyse médicale au sein d'un laboratoire, un patient a découvert que son médecin traitant avait accès à ses résultats par l'intermédiaire du site internet non sécurisé du laboratoire. Constatant également qu'il n'avait pas été informé du traitement de ses données personnelles et soupçonnant le laboratoire de n'avoir pas réalisé d'analyse d'impact, le patient a déposé une plainte auprès de l'autorité de contrôle belge.

En premier lieu, l'autorité de contrôle belge a précisé qu'un laboratoire d'analyses médicales doit être considéré comme un responsable du traitement. Effectivement, lors de la venue d'un patient, le laboratoire d'analyses médicales « détermine les finalités et les moyens du traitement » et ne reçoit pas d'instructions, nonobstant le fait que c'est un médecin qui prescrit l'analyse et « *envoie* » son patient réaliser lesdites analyses ;

En second lieu, l'autorité de contrôle a considéré que l'utilisation d'une page web non chiffrée (protocole http) sur laquelle apparaissaient les résultats d'analyse, viole le principe d'intégrité et de confidentialité inscrit aux articles 5.1.f et 32 du RGPD ;

Enfin, l'autorité de contrôle a estimé que le fait de placer des « *mentions RGPD* » directement dans les centres de prélèvement n'est pas suffisant au titre de l'information des personnes concernées dès lors que le laboratoire d'analyses médicales est amené à procéder à des analyses de patients qui ne se sont pas déplacés dans les locaux. Ainsi, elle considère qu'il appartient au laboratoire de publier une politique de confidentialité sur son site, sauf à violer les articles 12 à 14 du RGPD.

Compte tenu de ce qui précède, l'autorité de contrôle a prononcé une amende de 20.000 € à l'encontre du laboratoire d'analyse médicales pour avoir violé les articles 5.1.f ; 12 ; 13 ; 14 ; 32 et 35 du RGPD

**Source** : ici

VU DANS LA PRESSE

DSIH, 18 SEPTEMBRE 2023

# RECHERCHES MEDICALES : RAPPEL A L'ORDRE DE LA CNIL

*Parce que certains traitements présentent des risques « d'une ampleur particulièrement importante » (les traitements dits « critiques ») et qu'ils sont la cible « des attaquants qui disposent de fortes capacités ou de fortes motivations », la CNIL a rédigé un projet de recommandation relative aux modalités de sécurisation de ces traitements*[1].

**C'est quoi un traitement critique ?**

C'est un traitement qui répond aux deux conditions suivantes :

– Il est réalisé « à grande échelle » au sens du RGPD ;

– Il est celui pour lequel une violation de données pourrait soit entraîner des conséquences très importantes pour les personnes concernées, soit entraîner des conséquences pour la sûreté de l'État ou pour la société dans son ensemble (en raison de la perte de confidentialité, d'intégrité ou de disponibilité des données). Parmi les exemples de traitements critiques, la CNIL vise « les traitements de santé à grande échelle, aussi bien dans le cadre du soin, de la gestion des épidémies, de la recherche ou des mutuelles ».

**La nécessité d'une gouvernance de la protection des données personnelles**

Selon la CNIL, la protection des données personnelles concernées par des traitements critiques devrait se traduire par la mise en place d'une gouvernance dédiée.

A ce titre, l'autorité précise que la protection de telles données devrait être un « enjeu » porté par la direction générale de l'organisme, qui devrait s'assurer que les moyens suffisants sont mobilisés pour garantir la sécurité de ces traitements.

Par ailleurs, la CNIL estime que chaque organisme devrait désigner un référent en matière de protection des données personnelles et de sécurité pour le traitement concerné et se fixer des objectifs, (i) traduits en règles de fonctionnement et (ii) formalisés dans une politique de sécurité.

Elle ajoute que la sécurité devrait faire l'objet d'une « *démarche d'amélioration continue* », afin de permettre une « *progression constante* ».

Un bilan de sécurité pourrait être réalisé de manière annuelle pour « *tirer les leçons des éventuels incidents de sécurité* » et « *identifier et mettre en œuvre, sous la forme d'un plan d'action, les axes de progression* ».

**La nécessité d'une démarche de gestion des risques**

Pour la CNIL, les traitements critiques devraient « systématiquement » faire l'objet d'une analyse d'impact, avec une mise à jour régulière pour une prise en compte de l'évolution des risques.

Par ailleurs, la CNIL recommande que ces traitements fassent l'objet d'une homologation de sécurité avant leur mise en œuvre.

Cela consisterait à « *faire valider par la personne sous l'autorité de laquelle le traitement est mis en œuvre (par exemple, le directeur général dans une entreprise ou la personne délégataire du pouvoir de décision) le niveau de sécurité du traitement, les risques résiduels identifiés et le plan d'action visant à maintenir et à améliorer le niveau de sécurité du traitement dans le temps* ».

**La nécessité de cultiver une maturité élevée en sécurité et protection des données**

Selon la CNIL, il apparaît indispensable que les organismes concernés soient dotés d'un RSSI et d'équipes chargées d'inclure les problématiques de sécurité « *dans les phases amont des projets de modification ou de création de systèmes d'information, puis de maintenir la sécurité des systèmes dans le temps.* »

Cette maturité attendue par la CNIL suppose également que le personnel soit sensibilisé, de manière continue, à la sécurité informatique, à la protection des données, mais aussi aux nouvelles menaces.

Un exercice relatif à la sécurité informatique devrait être conduit régulièrement.

**La nécessité d'une démarche de défense en profondeur**

En application du concept de « *défense* en profondeur », la sécurité des données « *ne devrait pas être assurée par une mesure unique mais par un ensemble cohérent de mesures capables de parer à la défaillance d'une mesure unitaire* ».

La CNIL estime que, dans le cadre de cette démarche, les responsables du traitement devraient s'inspirer de la logique « *zéro confiance* », en tant que modèle d'architecture limitant la confiance implicite accordée au sein du système de défense périmétrique, tel que présenté par l'ANSSI.

Ce renforcement de la sécurité passerait par plusieurs mesures : cloisonnement, imputabilité, maîtrise des accès plus granulaires, analyse de la sécurité périmétrique, tests réguliers de restauration des sauvegardes, veille active des nouvelles vulnérabilités, etc.

**La nécessité d'une préparation active à d'éventuels incidents de sécurité ou violation de données**

La CNIL recommande que les traitements critiques fassent l'objet de « *mesures de traçabilité particulièrement poussées, mises en place dès l'intégration du traitement de données au système d'information et couvrant tous les équipements impliqués dans le traitement de données à caractère personnel* ». Elle ajoute que ces mesures de traçabilité devraient s'accompagner de « mesures d'analyse automatique des journaux afin de faciliter la détection des éventuels incidents de sécurité et violations de données ». Le responsable du traitement devrait, par exemple au moyen d'une procédure dédiée, préciser les critères conduisant à qualifier un incident de sécurité en tant que violation de données à caractère personnel. Par ailleurs, les organismes devraient être dotées d'un centre opérationnel de sécurité (COS ou SOC) disposant d'outils dédiés à l'analyse des journaux et à la détection d'incidents, et notamment d'un système de gestion des informations et des événements de sécurité. En fonction des risques pesant sur le traitement critique, le responsable devrait envisager que l'équipe de détection d'incident soit opérationnelle à tout instant.

**La nécessité d'une maîtrise des relations avec les tiers**

En plus d'un encadrement contractuel conforme aux exigences des articles 28 du RGPD et 122 de la loi « *informatique et libertés* », la CNIL estime que des exigences de sécurité devraient être formalisées et détaillées, notamment sous la forme de niveau de service attendu (SLA), « *à la hauteur des exigences que le responsable du traitement a identifiées pour le traitement* ».

De plus, la CNIL recommande qu'en fonction de la criticité de la prestation rendue par le sous-traitant, le responsable du traitement *« déploie des efforts proportionnés pour s'assurer du respect des obligations du contrat»*, en particulier sous la forme d'audits réguliers.

Ce projet est soumis à la consultation jusqu'au 8 octobre 2023 avec pour objectif la confirmation, d'une part, de la notion de « *traitements critiques* » et, d'autre part, des mesures de sécurité associées. Il est prévu que cette recommandation soit publiée au début de l'année 2024.

[1]https://www.cnil.fr/sites/cnil/files/2023-08/recommandation_relative_aux_traitements_critiques.pdf

**Lien vers l'article original** : ici

# UN LABORATOIRE D'ANALYSES MEDICALES INVOQUE SA QUALITE DE SOUS-TRAITANT POUR SE DEDOUANER DE TOUTE RESPONSABILITE

**VU DANS LA PRESSE**

**DSIH, 26 SEPTEMBRE 2023**

*Un patient s'est plaint du non-respect, par un laboratoire d'analyses médicales, de ses obligations au titre du RGPD. En défense, le laboratoire invoquait sa qualité de sous-traitant pour expliquer l'absence d'analyse impact et d'information des patients. Était-ce une bonne stratégie ?*

Les faits se déroulent en Belgique. A plusieurs reprises, un patient a réalisé, à la demande de son médecin, des analyses dans un laboratoire d'analyses médicales. Il est informé que son médecin pourra se procurer les résultats de ses analyses en se connectant sur le serveur de résultats « Cyberlab », accessible depuis le site internet du laboratoire. Constatant que ce serveur n'est pas sécurisé puisqu'accessible au moyen d'un protocole « http », le patient a déposé une plainte auprès de l'autorité de protection des données belge (ci-après l' « APD »).

Il invoquait également, à l'appui de sa plainte, d'autres manquements au RGPD : l'absence d'analyse d'impact (PIA) et l'absence d'information des personnes quant à l'utilisation des données par le laboratoire. Ce dernier contestait toute violation du RGPD, invoquant sa qualité de « *sous-traitant* ».

**Sur la qualification du laboratoire d'analyses médicales**

La stratégie du laboratoire était simple : puisque tous les manquements qui lui sont reprochés concernent des obligations qui incombent à un responsable du traitement et non à un sous-traitant, il a déclaré à l'autorité de contrôle être un sous-traitant au sens du RGPD. La circonstance selon laquelle les patients étaient envoyés par des médecins – responsables du traitement – devait contribuer, pensait-il, à appuyer sa thèse. Malheureusement, le laboratoire n'a pas réussi à convaincre le Service d'inspection de

Voyant sa stratégie vouée à l'échec, il a fini par reconnaître, dans ses conclusions de synthèse, sa qualité de responsable du traitement. La Chambre contentieuse, qui n'a pas hésité une seconde, a qualifié la partie défenderesse de responsable du traitement, compte tenu de la détermination, par cette dernière, des finalités et des moyens du traitement.

Même si on aurait souhaité que l'APD explique d'avantage son analyse, existait-il réellement un doute sur la qualification de responsable du traitement d'un laboratoire d'analyses médicales, y compris lorsque les analyses sont prescrites par un professionnel de santé ou même adressées par ce dernier au laboratoire ? Non, le doute n'était pas permis.

**Sur le défaut de sécurité du serveur de résultats**

Alors que le serveur de résultats du laboratoire, accessible depuis son site internet, permettait aux médecins d'accéder en temps réel aux résultats et à l'historique des analyses de leurs patients, le Service d'inspection a pu constater, comme le rapportait le plaignant, que ce serveur ne faisait l'objet d'aucun chiffrement puisqu'il utilisait un protocole « http » au lieu d'un protocole « https ».

Pour la Chambre contentieuse, l'absence de chiffrement au moment de la plainte constitue une violation du principe d'intégrité et de confidentialité des données, tel que prévu aux articles 5 et 32 du RGPD.

**Sur l'absence d'analyse d'impact**

Après avoir un moment soutenu, comme indiqué supra, qu'il n'était pas tenu de réaliser une analyse d'impact compte tenu de sa qualification de sous-traitant, le laboratoire a, une fois sa qualité de responsable du traitement reconnue, justifié l'absence d'un tel document au motif qu'il n'était pas contraint d'en rédiger un dès lors qu'au moment de la plainte, il ne traitait pas de données personnelles « *à grande échelle* ».

Il reconnaissait, en revanche, que, depuis le COVID-19, le nombre d'analyses avait sensiblement augmenté et qu'il rentrait désormais dans les conditions d'un traitement de données de santé à grande échelle, expliquant ainsi qu'il ait bien réalisé, depuis, une analyse d'impact.

Selon la Chambre contentieuse, il ne fait aucun doute que la partie défenderesse aurait dû, bien avant le COVID-19 (et donc avant que la plainte ne soit introduite), réaliser une analyse d'impact.

En tout de cause, elle aurait dû, ce qu'elle n'a pas fait, documenter les raisons pour lesquelles elle considérait ne pas être tenue de réaliser une telle analyse : « *Elle estime qu'elle effectue dorénavant des traitements à grande échelle*. *La défenderesse aurait dû, sur la base du principe de responsabilité de l'article 24, clarifier son interprétation de la notion de « grande échelle » en indiquant les critères objectifs sur lesquels elle se base pour estimer que ses activités ont fini par entrer dans la catégorie des traitements à grande échelle, alors que selon elle, elles ne remplissaient pas ce critère au départ.* »

**Sur l'information des patients**

Le dernier grief fait au laboratoire concernait l'absence de politique de protection des données disponible sur son site internet. Pour sa défense, le laboratoire a d'abord invoqué sa qualité de sous-traitant pour expliquer qu'il n'était pas tenu à la moindre obligation d'information à l'égard des patients. Puis, après avoir reconnu l'évidence, il soutenait qu'aucun manquement ne pouvait lui être reproché dès lors qu'un affichage était réalisé dans les centres de prélèvement et que le RGPD n'impose pas qu'une information soit publiée sur le site web.

Soulignant que le laboratoire ne rapportait pas la preuve que la politique de protection des données faisait l'objet d'un affichage dans ses centres de prélèvement, la Chambre contentieuse a considéré, qu'en ne publiant pas l'information requise sur son site internet, la partie défenderesse avait violé les articles 12, 13 et 14 du RGPD.

Malgré ces divers manquements, l'APD s'est montrée plutôt clémente en prononçant une amende administrative de 20.000 euros, correspondant à seulement 0,07% du chiffre d'affaires annuel du laboratoire pour l'année 2020[1].

[1] APD, 19 août 2022, 127/2022.

**Lien vers l'article original** : ici

VU DANS LA PRESSE

DSIH, 2 OCTOBRE 2023

# ENTREPOTS DE DONNEES DE SANTE : SYNTHESE ET ENJEUX

*Les 21 et 22 septembre 2023 s'est tenu le Salon-Congrès City Healthcare à la Cité des congrès de Nantes, consacré au numérique en santé. Cette 8e édition, organisée sous le haut patronage du ministre de la Santé et de la Prévention, était présidée par le Dr Lise Alter, directrice générale de l'Agence de l'innovation en santé.*

Au cours de ces deux journées entièrement dédiées au numérique en santé au travers de ses usages, plus de 140 experts et 70 exposants ont répondu présent. 40 tables rondes, conférences et workshops se sont tenus.

La thématique de l'une des tables rondes portait sur les entrepôts de données de santé (EDS). Plusieurs experts étaient réunis pour répondre aux questions suivantes : Pourquoi les entrepôts de données de santé sont-ils appelés à devenir de formidables outils de soins et de recherche ? Quel est leur impact direct sur les patients ? Par ailleurs, un focus a été réalisé sur le projet lauréat de l'appel à projets soutenu par France 2030 « ODH 2.0-GCS Hugo », à travers une illustration par cas d'usage.

Étaient présents les experts Caroline Dorphin (en charge des partenariats au sein du Health Data Hub), Me Delphine Ganoote Mary (avocate au barreau de Nantes et spécialiste du droit de la propriété intellectuelle, des nouvelles technologies, de l'informatique et de la communication), Fanny Gaudin (directrice de la recherche et de l'innovation au CHRU de Brest et déléguée générale du GCS Hugo), le Pr Marc Cuggia (médecin, professeur d'informatique médicale à l'université de Rennes 1 et directeur de l'équipe projet « Données massives en santé » à l'UMR Inserm 1099 LTSI – Laboratoire de traitement du signal et de l'image), le Pr Pierre-Antoine Gourraud (professeur des universités, praticien hospitalier au CHU de Nantes et responsable depuis 2018 de « La clinique des données », un nouveau service hospitalier dédié aux données générées par le soin au CHU de Nantes) et, enfin, Me Alexandre Fievée (avocat au sein du cabinet Deriennic Associés, spécialiste, entre autres, de l'innovation et des données, notamment dans le domaine de la santé).

Me Alexandre Fievée a accepté de revenir sur cet événement.

**De manière très simple, qu'est-ce qu'un EDS ?**

Un EDS peut être défini, en termes simples, comme la mise en commun des données d'un ou plusieurs systèmes informatiques médicaux, sous un format homogène, en vue d'une exploitation à d'autres fins, en principe, que celle pour laquelle elles ont été collectées.

Les données intégrées sont principalement des données administratives de patients et des données de santé (diagnostiques, de biologie, etc.). Ces données initialement collectées pour un usage primaire, c'est-à-dire dans le cadre de la prise en charge des patients, sont réutilisées pour d'autres finalités, telles que la recherche, mais aussi la production d'indicateurs d'activité pour le pilotage ou la qualité des soins. On parle d'une utilisation secondaire des données. Si les premiers EDS ont été conçus notamment pour optimiser le codage hospitalier à des fins de facturation, leur constitution a désormais pour finalité principale la recherche scientifique.

**Existe-il un cadre juridique spécifique à l'EDS ?**

D'un point de vue réglementaire, il convient de distinguer les règles en vigueur au titre de la constitution de la plateforme de celles qui sont applicables au cadre strict de la recherche.

S'agissant de la constitution de la plateforme, il est nécessaire de se rapporter au référentiel de la Cnil de 2021 qui énumère un certain nombre d'exigences en termes notamment de finalités, de règles de gouvernance, de gestion des droits d'accès, d'information des patients ou encore de sécurité. Si l'EDS entre dans le cadre de ce référentiel, une simple déclaration de conformité à la Cnil suffit. Dans le cas contraire, une demande d'autorisation à l'autorité de contrôle doit être déposée.

La réutilisation des données de santé à des fins de recherche doit en revanche être autorisée par la Cnil, sauf si elle s'inscrit dans le cadre d'une méthodologie de référence élaborée par la Commission. Dans ce dernier cas, un simple engagement de conformité à cette méthodologie suffit.

**Combien dénombre-t-on d'EDS en France ?**

Il est à relever que ce cadre réglementaire, qui pourrait s'apparenter à une contrainte, n'a pas fait obstacle au développement des EDS sur le territoire national. Un grand nombre

Il y a un an, on pouvait dénombrer plus de 30 CHU dotés d'un EDS, ce à quoi il faut ajouter toutes les autres structures de soins qui se sont également lancées dans une telle démarche.

**Quels sont les facteurs qui ont contribué au développement des EDS ?**

Cet écosystème a bénéficié incontestablement d'une accélération grâce à :

- des financements nationaux ;
- la multiplication d'acteurs industriels spécialisés en données de santé ;
- une réflexion supranationale à propos de l'espace européen des données de santé.

**Quels sont les enjeux de demain ?**

Si cet écosystème est en « *pleine expansion* », il est également, pour certains, « *sous-exploité* » en raison d'un financement insuffisant.

Pourtant, tout le monde s'accorde aujourd'hui à considérer que les données de santé détenues par les hôpitaux, les laboratoires d'analyses médicales et les professionnels de santé peuvent être déterminantes pour le développement de la recherche et de l'innovation en santé. D'un point de vue économique, les enjeux sont également considérables : une étude récente nous apprend que l'exploitation des données de santé représenterait un gain d'environ 7,3 milliards d'euros par an pour l'économie française.

Mais, selon le Health Data Hub, le financement actuellement consacré aux EDS est insuffisant pour favoriser leur pleine expansion. Il estime qu'une enveloppe globale annuelle de 60 à 90 millions d'euros serait indispensable pour le développement d'un réseau de 30 EDS de taille critique.

Peut-on dire [il s'agissait de l'une des questions posées dans le cadre de la table ronde] que les entrepôts de données de santé sont appelés à devenir de formidables outils de soins et de recherche ?

Absolument. Les EDS sont de formidables outils pour l'amélioration de la qualité des soins, de la recherche et de l'innovation. Mais encore faut-il que les financements suivent. Ces plateformes représentent incontestablement l'avenir, et leur développement va dans le sens des réflexions actuelles avec la création annoncée d'un espace européen des données de santé.

**Quel serait le mot de la fin ?**

N'oublions pas le patient. Il s'agit, avec le financement, d'un enjeu majeur. Maintenir la relation de confiance entre le corps médical et les patients est primordial, ce qui passe par un véritable effort pédagogique pour expliquer aux patients les finalités d'un EDS et les objectifs de l'utilisation secondaire de leurs données. Il faut aussi leur rappeler qu'ils ont des droits et que les mesures nécessaires ont été mises en œuvre pour garantir la sécurité de leurs données.

**Lien vers l'article original** : ici