

Gestion d'entrepôt de données de santé : la CNIL sanctionne IQVIA à hauteur de 5 millions d'euros

Clarence Tocchio, le 20 août 2026

La CNIL rend une décision majeure relative aux entrepôts de données de santé, dans un contexte marqué par l'entrée en vigueur du règlement relatif à l'Espace européen des données de santé et par les enjeux croissants liés à l'anonymisation des données, notamment à la suite de la publication des lignes directrices du CEPD en la matière. Elle rappelle à cette occasion que l'autorisation délivrée pour la création d'un entrepôt de données de santé fixe le périmètre et les conditions de traitement, dont le respect doit être assuré de manière continue par le responsable de traitement. Le non-respect de ces conditions, même en l'absence d'observation préalable de la CNIL, est susceptible de caractériser un manquement au RGPD et/ou à la LIL et d'entraîner une sanction.

Délibération de la formation restreinte n°SAN-2026-008 du 26 mai 2026 concernant la société IQVIA OPERATIONS FRANCE

Introduction

La Commission nationale de l'informatique et des libertés (CNIL) sanctionne le non-respect des autorisations qu'elle a délivrées à la société IQVIA OPERATIONS France (IQVIA) (filiale du groupe étatsunien IQVIA) pour deux entrepôts de données de santé. Plus spécifiquement, la CNIL offre son analyse des exigences nationales relatives aux traitements de données de santé (art. 66 Loi Informatique et Libertés), à l'information des personnes en cas de collecte indirecte de données (art. 14 RGPD) et à la protection des données dès la conception et par défaut (art. 25 RGPD).

Faits

Afin d'analyser l'activité des pharmacies (aussi appelées « officines ») ainsi que le suivi des parcours de soins des patients, la société IQVIA a reçu deux autorisations de la CNIL pour créer des entrepôts de données de santé. D'une part, l'entrepôt *Longitudinal prescription data* (LRX), alimenté par des données collectées auprès d'officines et autorisé par la délibération n°2018-289 du 12 juillet 2018. Ce dernier a pour vocation de collecter auprès d'environ

14 000 officines partenaires, les données liées aux ventes de médicaments avec la création d'un code d'identification unique et identique quelle que soit l'officine partenaire, permettant un suivi du parcours de chaque patient. Les données sont par la suite pseudonymisées et en contrepartie, la société transmet aux officines partenaires, un tableau de bord de leurs données de vente afin de pouvoir comparer leur activité à celle d'autres officines et de gérer leur stock. D'autre part, l'entrepôt *Electronic medical records* (EMR), alimenté par des données collectées auprès de médecins et autorisé par la délibération n°2021-015 du 4 février 2021. Il a quant à lui pour objectif de collecter des données auprès de médecins, avec un identifiant propre à chaque patient mais qui diffère pour chaque médecin. Les données sont également pseudonymisées et en contrepartie, les médecins peuvent bénéficier des publications réalisées par la société et participer à des études.

À la suite de la diffusion d'un reportage portant notamment sur les données à caractère personnel traitées par la société IQVIA, la CNIL a reçu de nombreuses plaintes et signalements la conduisant à publier un communiqué rappelant les règles applicables et les garanties exigées à IQVIA. Ultérieurement, la CNIL a réalisé un contrôle sur place afin de vérifier la conformité des traitements réalisés par IQVIA à la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (LIL) et au RGPD. Il en ressort plusieurs manquements à l'article 66 LIL (obligation de respecter les autorisations délivrées par la CNIL), un manquement à l'article 14 RGPD (information des personnes s'agissant de l'entrepôt LRX) et un manquement à l'article 25 RGPD (protection des données dès la conception et par défaut).

Droit

Pour rappel, lorsqu'un responsable de traitement souhaite créer une base de données comportant des données de santé, ce dernier doit déterminer en amont si l'objectif est la réalisation ultérieure de plusieurs traitements ou la recherche, l'étude ou l'évaluation ponctuelle. Cela est déterminant puisque le régime juridique et les formalités applicables diffèrent selon les situations (demande d'autorisation « santé » auprès de la CNIL incluant une AIPD, engagement de conformité à la méthodologie de référence, etc.).

La CNIL détaille principalement son analyse en trois parties : (i) la responsabilité de la société et la nature des données traitées, (ii) les manquements liés à l'entrepôt LRX et (iii) les manquements liés à l'entrepôt EMR.

(i) La responsabilité de la société et la nature des données traitées

Se prévalant de la jurisprudence *EDPS vs SRB* (commentée in <https://swissprivacy.law/385/>), IQVIA argue que les données présentes dans ses entrepôts ne doivent pas être considérées comme des données à caractère personnel. La CNIL conteste cette argumentation en retenant que les mesures de pseudonymisation mises en place par IQVIA, responsable de traitement, ne sont pas aptes à supprimer les risques de réidentification.

Concernant la qualification de responsable de traitement eu égard aux traitements mis en œuvre dans le cadre de la constitution des entrepôts LRX et EMR, la CNIL rappelle qu'aux termes de l'art. 4 ch. 7 RGPD, le responsable de traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ». Les lignes directrices 07/2020 du CEPD concernant les notions de responsable du traitement et de sous-traitant précisent que le responsable du traitement est l'acteur qui a déterminé la raison pour laquelle le traitement a lieu et comment cet objectif sera atteint.

En l'espèce, la CNIL relève que IQVIA a été autorisée à procéder à la constitution des entrepôts LRX et EMR en qualité de responsable de traitement sur le fondement des intérêts légitimes de cette dernière. Concernant l'entrepôt EMR, la CNIL souligne que la notice d'information à destination des patients est élaborée par IQVIA et que cette dernière se présente comme responsable de l'ensemble des opérations. Par conséquent, la CNIL retient que IQVIA détermine la finalité et les moyens de ces deux entrepôts et doit être considérée comme responsable de traitement de l'ensemble des opérations mises en œuvre dans le cadre de ces derniers.

Pour ce qui est du caractère personnel des données traitées, la CNIL rappelle que l'art. 4 al. 1 et 5 RGPD et le considérant 26 RGPD fournissent des éléments d'appréciation quant au caractère identifiable et s'appuie sur la jurisprudence de la CJUE, notamment l'arrêt *EDPS vs SRB* (C-413/23 du 4 septembre 2025, commenté in <https://swissprivacy.law/385/>) qui précise que des données pseudonymisées ne sont pas considérées comme des données à caractère personnel au sens du RGPD si le destinataire n'est pas en capacité de lever les mesures et que lors d'un recoupement avec d'autres éléments, la personne concernée n'est pas ou plus identifiable. Enfin, la CNIL soutient son argumentaire à l'aide d'une décision du Conseil d'État français qui indique, à propos de données figurant dans des bases alimentées par des données collectées auprès de médecins et d'officines pharmaceutiques, qu'il est « possible, (...) de retracer des parcours de soins et d'individualiser des clients et leurs pathologies » par des moyens raisonnables et qu'il s'agit par conséquent de données à caractère personnel (cf. CE du 13 février 2026, n°498628).

En l'espèce, IQVIA n'est pas un simple destinataire mais responsable du traitement, car la société détermine les finalités comme les moyens du traitement, de sorte que cette qualification fait obstacle à ce que les données puissent être considérées comme anonymes. En effet, l'intention, l'intérêt ou la motivation du responsable de traitement ou du tiers à réidentifier les personnes concernées, ne sont pas des facteurs pertinents à prendre en considération pour apprécier le caractère personnel ou non d'un ensemble de données. De surcroît, en raison de l'accumulation d'informations sur la prise en charge de patients ainsi que la possibilité de les individualiser, mais également compte tenu de la richesse des informations que ces entrepôts contiennent, la CNIL retient à juste titre que des risques de réidentification réels sont présents. Dès lors, les données figurant dans les entrepôts LRX et EMR doivent être considérées comme des données à caractère personnel, soumises au RGPD et à la LIL.

(ii) Les manquements liés à l'entrepôt LRX

Pour l'entrepôt LRX, la CNIL retient plusieurs manquements aux art. 66 LIL et 14 et 25 RGPD. Afin de justifier le manquement à l'obligation de respecter l'autorisation délivrée par la CNIL dans le domaine de la santé en matière de recherche (art. 66 LIL), cette dernière rappelle les principes posés par l'art. 32 RGPD concernant la sécurité du traitement et se focalise sur le cloisonnement du réseau et la traçabilité des accès. S'agissant du cloisonnement du réseau, il est fait référence au guide d'hygiène informatique publié en janvier 2017 par l'Autorité française en matière de cybersécurité et de cyberdéfense (ANSSI) qui précise que pour sécuriser un réseau, il convient de le segmenter et de mettre en place un mécanisme de cloisonnement. Or, il est reproché à IQVIA l'absence de cloisonnement du réseau pour limiter l'accès à la base de données de l'entrepôt LRX ainsi que l'absence de politique d'authentification multifacteur alors que le cloisonnement du réseau était expressément exigé par l'autorisation délivrée par la CNIL. S'agissant de la traçabilité des accès, la CNIL rappelle que la mise en place d'un dispositif de journalisation participe au respect de l'obligation de sécurisation de tout traitement (cf. Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation), qu'« un contrôle des traces doit être réalisé régulièrement et a minima bimestriellement, ainsi qu'à la fin de chaque période d'habilitation liée à un projet de recherche » (cf. Référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé), et « que le système de journalisation doit concerner non seulement les anomalies et événements liés à la sécurité, mais également les activités métier des utilisateurs et les interventions techniques » (cf. CNIL, Sécurité : Tracer les opérations).

En l'espèce, bien que IQVIA ait mis en place un système permettant de détecter d'éventuels

comportements anormaux ou mésusages des données (SIEM), la CNIL sanctionne plus généralement le fait de ne pas avoir mis en place un dispositif permettant une analyse régulière des journaux de connexion.

La CNIL met également en exergue le fait que les études réalisées par la société et pour son propre compte ne font l'objet d'aucune autorisation. D'une part, ces dernières sont exclues du champ de l'autorisation délivrée pour l'entrepôt LRX. D'autre part, elles ne sont conformes à aucun référentiel applicable.

En effet, si une société souhaite réaliser des études, évaluations ou recherches à partir de données à caractère personnel, cette dernière doit déposer auprès de la CNIL une déclaration de conformité au référentiel de méthodologie de référence MR-004. Cependant, pour qu'une société puisse s'en prévaloir, un certain nombre de conditions doivent être respectées, telles que l'affichage d'une information générale et la délivrance de l'information de manière individuelle aux personnes concernées. En l'espèce, la CNIL retient que les personnes concernées n'étaient ni informées de cette collecte ni de la réutilisation de leurs données dans le cadre des études réalisées par la société. Eu égard à ces éléments, la CNIL retient que IQVIA ne respecte pas les termes de l'autorisation, ce qui constitue un manquement à l'[art. 66 LIL](#).

Concernant l'obligation de fournir des informations lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, l'[art. 14 RGPD](#) pose le principe selon lequel, dès lors qu'un responsable du traitement ne collecte pas des données à caractère personnel auprès de la personne concernée, ce dernier doit lui fournir un grand nombre d'informations telles que son identité, la durée de conservation, les finalités du traitement, etc.

En l'espèce, la CNIL rappelle que dans la délibération concernant l'entrepôt LRX, il est indiqué que « les pharmaciens d'officine seront chargés, contractuellement, d'informer individuellement leurs clients du traitement des données les concernant ». Cependant, sur les officines contrôlées, aucune d'entre elles ne délivraient lesdites informations. Par conséquent, la CNIL impute ce manquement à IQVIA en raison de sa qualité de responsable de traitement.

Pour ce qui est de la protection des données dès la conception et par défaut, la CNIL rappelle les obligations présentées à l'[art. 25 RGPD](#) ainsi que le principe clarifié dans les [lignes directrices 4/2019](#) y relatives (dans leur seconde version) selon lequel les données à caractère personnel doivent être protégées dès la conception du traitement et par défaut.

En l'espèce, il est reproché à la société que les modules d'extraction de données des pharma-

ciens transmettent systématiquement au premier tiers de confiance les données des patients. La CNIL retient ainsi que cette transmission n'est pas justifiée et que IQVIA aurait dû prévoir, dès la conception et par défaut, des mesures permettant de s'assurer que les logiciels n'extraient pas les données des patients lorsque le pharmacien refuse cette communication.

(iii) Les manquements liés à l'entrepôt EMR

Pour l'entrepôt EMR, la CNIL retient également un manquement à l'art. 66 LIL en raison de manquements liés à l'information des patients, l'exercice des droits, la sécurité et confidentialité des données.

Sur l'information des patients, la CNIL rappelle les obligations prévues par l'art. 14 RGPD (cf. *supra*). Dans le cas d'espèce, l'autorisation délivrée par la CNIL à IQVIA indiquait que les données de l'entrepôt EMR « seront conservées en base active pendant une durée de dix ans. Au-delà, les données seront anonymisées ou supprimées ». Or, la notice destinée à informer les patients des traitements mis en œuvre ne mentionnait pas les mêmes informations puisqu'elle indiquait que les données sont conservées pendant la durée de réalisation des études et analyses mises en œuvre par IQVIA et ses partenaires contractuels, avant de faire l'objet d'une procédure d'archivage sécurisée pour une durée conforme à la réglementation en vigueur.

Néanmoins, il convient de souligner que IQVIA avait soumis ladite notice à la CNIL dans le cadre de sa demande d'autorisation et que cette dernière n'avait soulevé aucune interrogation. Désormais, la CNIL retient que les informations fournies dans la notice litigieuse ne correspondent ni à la durée prévue par l'autorisation, ni à celle pratiquée par IQVIA.

Quant à l'exercice des droits, il est reproché à IQVIA de n'avoir prévu aucun mécanisme *a posteriori* permettant la levée du pseudonymat et la réidentification effective des personnes concernées pour permettre la prise en compte de leur droit d'opposition. IQVIA se prévaut du fait que cela apparaît techniquement impossible et que si une telle demande doit avoir lieu, la personne concernée doit renseigner un certain nombre d'informations afin que IQVIA puisse tenter de réidentifier le patient. Toutefois, la CNIL considère que dans la mesure où IQVIA conditionne la prise en compte du droit d'opposition du patient à la fourniture d'informations complémentaires, cela n'est ni conforme au RGPD, ni à l'autorisation qu'elle a délivrée.

Pour ce qui est de la sécurité et de la confidentialité des données, la CNIL relève, en sus de

l'absence de cloisonnement du réseau et de traçabilité des accès, qu'aucun mécanisme d'authentification forte ou multifacteur n'est implémenté s'agissant de l'accès à l'entrepôt et qu'un seul jeu d'identifiant/authentifiant était suffisant pour s'authentifier. Par conséquent, IQVIA a violé l'[art. 66 LIL](#).

Conclusion

Cette délibération sur la gouvernance des entrepôts de données de santé rappelle que le respect des formalités préalables ne constitue pas une simple exigence administrative, mais bien une condition essentielle à la licéité du traitement. Elle met en évidence la nécessité de distinguer les informations présentées par le responsable de traitement dans sa demande d'autorisation, des obligations qui résultent de l'autorisation délivrée par la CNIL. En effet, si la demande permet d'exposer le projet ainsi que les garanties envisagées, seule l'autorisation délivrée par la CNIL fixe le périmètre du traitement, les finalités ainsi que les obligations auxquelles le responsable de traitement sera tenu de se conformer. Toute divergence est ainsi susceptible de caractériser un manquement au RGPD et/ou à la LIL.

De plus, l'obtention d'une autorisation ne marque pas la fin de la démarche de conformité, mais le point de départ d'une obligation permanente de veiller au respect des engagements pris auprès de la CNIL. Les responsables de traitement doivent ainsi mettre en place des mécanismes de contrôle interne permettant de s'assurer que les traitements réalisés, les données collectées, les destinataires, les durées de conservation ou encore les mesures de sécurité demeurent conformes aux conditions énoncées dans l'autorisation.

Finalement, cette décision illustre que l'absence de réaction de la CNIL à la réception d'un document ne saurait être assimilée à une validation tacite de son contenu, ni faire obstacle à une sanction ultérieure. La CNIL étant composée de différents services, le service en charge de l'instruction des demandes d'autorisation pour les entrepôts de données de santé est distinct de celui des contrôles et sanctions. Le silence ou l'absence de remarque d'un service ne saurait ainsi lier et/ou limiter l'appréciation de la formation restreinte chargée de prononcer, *a posteriori* et de manière autonome, des sanctions en raison de la non-conformité d'un traitement au RGPD ou à la LIL.

Par conséquent, au-delà du risque de sanction financière, le non-respect des conditions de l'autorisation est susceptible d'entraîner une remise en cause de l'autorisation délivrée par la CNIL, un préjudice réputationnel ainsi qu'une perte de confiance des personnes concernées comme des partenaires. La conformité ne se limite pas à l'obtention d'une autorisation de la CNIL mais suppose le respect strict et continu des obligations figurant dans la décision d'auto-

risation tout au long de la vie du traitement.

Proposition de citation : Clarence Тосчио, Gestion d'entrepôt de données de santé : la CNIL sanctionne IQVIA à hauteur de 5 millions d'euros, 20 août 2026 *in* www.swissprivacy.law/415

 Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.