# CHECK-LIST DE CONFORMITÉ

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

# Introduction

La check-list suivante permet de vous guider afin de vérifier la stricte conformité du traitement de données au référentiel relatif aux traitements de données personnelles mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé.

**Toute réponse négative (« faux ») à l'une des questions signifie que le traitement envisagé n'est pas conforme au référentiel.**

Tout traitement qui ne respecte pas l'ensemble des exigences définies par le référentiel doit faire l'objet d'une autorisation spécifique par la CNIL afin d'être mis en œuvre. L'autorisation ne pourra être délivrée que si le traitement est suffisamment protecteur des données des personnes concernées et si des mesures supplémentaires sont mises en œuvre afin de compenser les points de non-conformité au référentiel.

Voir la rubrique 2. « Portée du référentiel » pour le détail des modalités à réaliser.

Le référentiel ne s'applique pas :

- aux entrepôts mis en œuvre par une société privée sur le fondement de son intérêt légitime ;
- aux traitements de données personnelles mis en œuvre uniquement aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par les professionnels de santé et les systèmes ou services de soins de santé (p. ex : les dossiers médicaux dématérialisés). Ces traitements ne nécessitent pas de formalités préalables auprès de la CNIL ;
- aux traitements de données personnelles mis en œuvre lorsque la personne a donné son consentement explicite à cette fin. Ces traitements ne nécessitent pas de formalités préalables auprès de la CNIL ;
- aux entrepôts appariés avec la base principale du Système national des données de santé (SNDS) tel que défini à l'article L. 1461-1 du code de la santé publique.

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **1. À qui s'adresse ce référentiel** | | | |
| **1.3** | L'entrepôt envisagé entre dans le champ d'application du référentiel (voir les quatre situations dans lesquelles le référentiel ne s'applique pas en page précédente). | ☐ Vrai<br>☐ Faux<br>*Si « faux » : non-conformité au référentiel* | |
| **3.1. Finalités** | | | |
| **3.1.1** | L'entrepôt est mis en œuvre afin de permettre la réutilisation des données qu'il contient (recherche, évaluations, calcul d'indicateurs, etc.). | ☐ Vrai<br>☐ Faux | |
| **3.1.2** | Toute utilisation uniquement des données de l'entrepôt par le responsable de traitement et pour son usage exclusif, l'est à des fins de :<br>• production d'indicateurs et le pilotage stratégique de l'activité, sous la responsabilité du médecin responsable de l'information médicale ;<br>• amélioration de la qualité de l'information médicale ou l'optimisation du codage dans le cadre du programme de médicalisation des systèmes d'information (PMSI) ;<br>• fonctionnement d'outils d'aide au diagnostic médical ou à la prise en charge ;<br>• réalisation d'études de faisabilité (pré-screening) ;<br>• réalisation de recherches, études et évaluations dans le domaine de la santé.<br><br>En dehors des utilisations mentionnées ci-dessus, le responsable de traitement doit s'interroger sur la nécessité ou non de réaliser des formalités spécifiques auprès de la CNIL pour toute réutilisation des données. | ☐ Vrai<br>☐ Faux | |
| **3.1.4** | Les données ne sont et ne seront pas exploitées :<br>• à des fins de promotion des produits mentionnés au II de l'article L. 5311-1 CSP en direction de professionnels de santé ou d'établissements de santé ;<br>• à des fins d'exclusion de garanties des contrats d'assurance, ni de modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque | ☐ Vrai<br>☐ Faux | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **3.2. Gouvernance** | | | |
| **3.2.1** | Une gouvernance est prévue pour organiser et encadrer le fonctionnement de l'entrepôt (au besoin avec des instances mutualisées si le responsable de traitement souhaite mettre en œuvre plusieurs entrepôts de données différents). | ☐ Vrai<br>☐ Faux | |
| **3.2.2** | Une première instance (comité de pilotage ou équivalent) détermine les orientations stratégiques et scientifiques de l'entrepôt.<br>Cette instance :<br>• tient une liste exhaustive des données de l'entrepôt et justifie de leur nécessité ;<br>• fait intervenir un DIM ainsi qu'un représentant de la conférence ou de la commission médicale d'établissement (si applicable). | ☐ Vrai<br>☐ Faux | |
| **3.2.3** | Une seconde instance (comité scientifique et éthique, ou équivalent) rend, de manière systématique, un avis préalable et motivé sur les propositions de projets nécessitant la réutilisation des données de l'entrepôt.<br>• seuls les projets ayant été examinés peuvent avoir recours à l'entrepôt, et l'avis de la seconde instance est communiqué sans délai au porteur de projet ;<br>• une liste des traitements sur lesquels le comité s'est prononcé est communiquée de façon périodique, au moins une fois par an, au délégué à la protection des données du responsable de traitement. | ☐ Vrai<br>☐ Faux | |
| **3.2.3.4** | Cette seconde instance (comité scientifique et éthique, ou équivalent) est composée :<br>• d'au moins une personne impliquée dans l'éthique en santé ;<br>• d'une personne indépendante du responsable de traitement ;<br>• de professionnels de santé et professionnels médico-sociaux ;<br>• de chercheurs ;<br>• d'un représentant des usagers ou d'une association de patients. | ☐ Vrai<br>☐ Faux | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **4. Base(s) légale(s) du traitement** | | | |
| **4.** | L'entrepôt permet au responsable de traitement d'exercer sa ou ses mission(s) d'intérêt public (base légale du traitement - article 6-1-e du RGPD).[1] | ☐ Vrai<br>☐ Faux | |
| **5. Données personnelles pouvant être incluse dans l'entrepôt** | | | |
| **5.1** | Les données collectées et traitées par le responsable de traitement sont uniquement :<br>• des données figurant dans le dossier médical et administratif ou dossier unique informatisé de la personne concernée et dont la collecte est justifiée par sa prise en charge et/ou ;<br>• des données issues de projets de recherches, études et évaluations dans le domaine de la santé précédemment réalisés et dont leur durée de conservation n'a pas expiré. | ☐ Vrai<br>☐ Faux | |
| **5.2.1.1** | Les données directement identifiantes éventuellement collectées mentionnées au point 5.2.1.1 sont conservées dans un espace distinct des autres données. | ☐ Vrai<br>☐ Faux<br>☐ N/A<br>(si aucune donnée directement identifiante n'est collectée) | |
| **5.2.1.2** | Aucune donnée sensible, autre que celles mentionnées au point 5.2.1.2, n'est collectée. | ☐ Vrai<br>☐ Faux | |
| **5.2.2** | Aucune donnée concernant les professionnels, autre que celles mentionnées au point 5.2.2., n'est collectée. | ☐ Vrai<br>☐ Faux | |
| **5.3** | La collecte initiale des données est scientifiquement justifiée par la prise en charge sanitaire ou médico-sociale ou par la réalisation d'un projet de recherche, d'étude ou d'évaluation spécifique et prévue par un protocole. | ☐ Vrai<br>☐ Faux | |
| **5.3** | Aucune donnée n'est collectée uniquement afin d'alimenter l'entrepôt. | ☐ Vrai<br>☐ Faux | |

[1] Attention : le caractère d'intérêt public de la mission du responsable de traitement doit être distingué de l'exigence d'intérêt public imposée pour les finalités des traitements mis en œuvre dans le domaine de la santé, conformément à l'article 66 de la loi Informatique et Libertés.

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **5.4** | Pour toute réutilisation, la nécessité de traiter des données de l'entrepôt est justifiée, pour chaque catégorie, dans la demande soumise à l'instance compétente de gouvernance de l'entrepôt. | ☐ Vrai<br>☐ Faux | |
| **5.5** | Les données directement identifiantes mentionnées au 5.2.1.1. du référentiel sont réunies dans l'entrepôt uniquement afin :<br>• de recontacter les patients pour leur proposer de participer à des études ultérieures ou pour les informer des projets de recherche réutilisant leurs données comprises dans l'entrepôt ;<br>• de recontacter les patients suite à la découverte de caractéristiques génétiques pouvant être responsables d'une affection justifiant des mesures de prévention ou de soins à leur bénéfice ou au bénéfice de leur famille, à l'exception des cas dans lesquels le patient s'y est opposé ;<br>• de recontacter les patients à la suite de découvertes annexes liées à l'identification de facteurs de risques et/ou d'identification syndromiques à même de modifier leur prise en charge ;<br>• avertir une personne d'un risque sanitaire auquel elle est exposée. | ☐ Vrai<br>☐ Faux<br>☐ N/A<br>(si aucune donnée directement identifiante n'est collectée) | |
| **5.6** | Les données directement identifiantes mentionnées au 5.2.1.1. ne sont utilisées que pour des finalités justifiées par le responsable de traitement.<br>Par exemple, l'information relative au jour de naissance d'une personne peut être collectée si la réalisation d'une recherche est conditionnée à un critère d'âge. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si aucune donnée directement identifiante n'est collectée) | |
| **5.7** | La pertinence des données comprises dans l'entrepôt est ré-évaluée régulièrement par l'instance compétente de gouvernance.<br>Cette pertinence s'apprécie au regard des projets menés et envisagés. | ☐ Vrai<br>☐ Faux | |
| **5.7** | Les données n'apparaissant plus nécessaires seront supprimées. | ☐ Vrai<br>☐ Faux | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **5.8** | Sont stockées séparément des données pseudonymisées et en utilisant les procédés décrits dans les exigences de sécurité SEC-LOG-4 à SEC-LOG-6 :<br>• les données directement identifiantes ;<br>• les tables de correspondance ;<br>• les données génétiques ;<br>• les données de suivi de localisation. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si ces catégories de données ne sont pas collectées) | |
| **6. Accès aux informations** | | | |
| **6.1** | Une attention particulière est prêtée à la gestion des droits d'accès des personnes habilitées à accéder aux données contenues dans l'entrepôt. | ☐ Vrai<br>☐ Faux | |
| **6.2** | L'accès et l'usage des données directement identifiantes sont restreints aux finalités listées au point 5.5 et aux seules personnes chargées de la réalisation des opérations nécessaires à l'accomplissement de ces finalités. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si aucune donnée directement identifiante n'est collectée) | |
| **6.3** | Seules des équipes de recherche habilitées sont destinataires des données pseudonymisées (internes ou externes au responsable de traitement).<br>Les données mises à leur disposition sont strictement nécessaires à la réalisation des objectifs de leurs projets de recherche, d'étude ou d'évaluation. | ☐ Vrai<br>☐ Faux | |
| **6.4** | En dehors des équipes de recherche, seul le personnel interne au responsable de traitement habilité est destinataire des données pseudonymisées.<br>Les données mises à leur disposition sont strictement nécessaires à l'accomplissement de leurs missions. | ☐ Vrai<br>☐ Faux | |
| **7. Durées de conservation** | | | |
| **7.1** | La durée de conservation des données répond aux critères énoncés à l'article 5.1.e du RGPD :<br>• les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au | ☐ Vrai<br>☐ Faux | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| | regard des finalités pour lesquelles elles sont traitées ;<br>• les données peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation). | | |
| **7.2** | Les données mentionnées au 5.2.1.2 (données sensibles des personnes concernées) sont supprimées au plus tard 20 ans après leur collecte dans le cadre des soins ou des recherches. | ☐ Vrai<br>☐ Faux | |
| **7.2** | Les données mentionnées au 5.2.1.1 (données identifiantes des personnes concernées) sont supprimées lorsque le délai de conservation des données sensibles (du point 5.2.1.2) a expiré, et au plus tard 20 ans après leur collecte. | ☐ Vrai<br>☐ Faux | |
| **7.3** | A l'issue de ces durées, les données sont anonymisées ou détruites. | ☐ Vrai<br>☐ Faux | |
| **8. Information des personnes** | | | |
| **8.1** | Une information des personnes dont les données ont été collectées lors de leur prise en charge concernant la constitution et le versement de leurs données dans l'entrepôt est prévue. | ☐ Vrai<br>☐ Faux | |
| **Informations auprès des patients admis ou réadmis postérieurement à la constitution de l'entrepôt** | | | |
| **8.2.2.1** | Les nouveaux patients, ainsi que ceux en cours de suivi, sont informés individuellement de la constitution de l'entrepôt. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de patients admis postérieurement à la constitution de l'entrepôt) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **8.2.2.1** | La note d'information à destination des personnes contient toutes les informations mentionnées à l'article 13 du RGPD. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de patients admis postérieurement à la constitution de l'entrepôt) | |
| **8.2.2.2** | La note d'information met en avant la réutilisation des données ainsi que les modalités d'exercice des droits d'accès et d'opposition. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de patients admis postérieurement à la constitution de l'entrepôt) | |
| **Informations auprès des patients admis antérieurement à la constitution de l'entrepôt et n'étant plus suivis** | | | |
| **8.2.3.1** | Les patients admis antérieurement à la constitution de l'entrepôt et n'étant plus suivis sont informés individuellement de la constitution de l'entrepôt.<br>Si les patients ne peuvent être informés individuellement, le responsable de traitement invoque une dérogation à l'information individuelle (points 8.2.3.4 et 8.2.3.5) et prévoit une information collective (point 8.2.3.6). | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de patients admis antérieurement à la constitution de l'entrepôt) | |
| **8.2.3.1** | La note d'information à destination des personnes contient toutes les informations mentionnées à l'article 14 du RGPD. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de patients admis antérieurement à la constitution de l'entrepôt) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| 8.2.3.3 | La note d'information met en avant la réutilisation des données ainsi que les modalités d'exercice des droits d'accès et d'opposition. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de patients admis antérieurement à la constitution de l'entrepôt) | |
| 8.2.3.4 et 8.2.3.5 | En cas de demande d'exception à l'obligation d'information individuelle pour la constitution de l'entrepôt, la dérogation invoquée par le responsable de traitement est justifiée par le fait que la fourniture de l'information exigerait un effort disproportionné, fondé par exemple sur :<br>• le nombre de personnes concernées ;<br>• l'ancienneté des données ;<br>• l'absence d'adresse postale ou électronique parmi les données détenues par le responsable de traitement ;<br>• le coût et le temps de la délivrance des informations<br><br>Par ailleurs l'exception invoquée ne s'applique qu'aux catégories de personnes pour laquelle la fourniture l'information exigerait un effort disproportionné. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de patients admis antérieurement à la constitution de l'entrepôt) | |
| 8.2.3.5 | Afin de pallier l'absence d'information individuelle, des mesures sont prévues et mises en œuvre afin de protéger les droits et libertés ainsi que les intérêts légitimes des personnes concernées. Ces mesures sont détaillées dans l'AIPD. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de patients admis antérieurement à la constitution de l'entrepôt) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| 8.2.3.6 | En l'absence d'information individuelle (pour l'ensemble comme pour une partie des personnes concernées), une information est rendue publiquement disponible, par exemple :<br>• par la diffusion d'une note d'information relative à la constitution de l'entrepôt sur le site web du responsable de traitement, dans une rubrique dédiée et accessible, complétée par des informations détaillées sur chaque traitement mis en œuvre à partir de l'entrepôt ;<br>• par la mise en place d'un « portail de transparence » sur le site web du responsable de traitement (entrepôt et réutilisations ultérieure des données) ;<br>• par des communications au sujet de l'entrepôt sur les réseaux sociaux, médias régionaux, associations de patients ;<br>• par la diffusion d'un communiqué de presse informant de la mise en place de cet entrepôt. | ☐ Vrai<br>☐ Faux<br>☐ N/A<br>(si l'entrepôt ne contient pas de données de patients admis antérieurement à la constitution de l'entrepôt) | |
| **Informations des personnes concernées par des projets de recherche dont les données sont incluses dans l'entrepôt** | | | |
| 8.3.1 | Les personnes dont les données issues de recherches sont intégrées à l'entrepôt sont informées individuellement de cette réutilisation de leurs données, conformément aux dispositions de l'article 14 RGPD. | ☐ Vrai<br>☐ Faux<br>☐ N/A<br>(si l'entrepôt ne contient pas de données issues de recherches) | |
| 8.3.1 | En cas de recours à l'exception à l'obligation d'information individuelle, les conditions détaillées aux points 8.2.3.4 à 8.3.2.6 sont respectées. | ☐ Vrai<br>☐ Faux<br>☐ N/A<br>(si l'entrepôt ne contient pas de données issues de recherches) | |
| 8.3.2 | La durée de conservation des données issues de la recherche n'a pas expiré. | ☐ Vrai<br>☐ Faux<br>☐ N/A<br>(si l'entrepôt ne contient pas de données issues de recherches) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **Informations des personnes concernées de chacune des réutilisations des données de l'entrepôt** | | | |
| **8.4** | Le responsable de traitement met en place un « portail de transparence » sur son site internet, informant les personnes concernées des projets de recherche réutilisant leurs données comprises dans l'entrepôt.<br>Les notes d'information des patients renvoient vers ce portail de transparence. | ☐ Vrai<br>☐ Faux | |
| **8.4** | Les personnes concernées sont informées de chacune des réutilisations des données les concernant à des fins de recherche, d'étude ou d'évaluation. Cette information peut se faire *via* le « portail de transparence » | ☐ Vrai<br>☐ Faux | |
| **Informations des professionnels** | | | |
| **8.5.1** | Les professionnels exerçant au sein des établissements du responsable de traitement postérieurement à la mise en œuvre de l'entrepôt et dont les données sont versées à l'entrepôt sont informés de façon individuelle et par écrit de toutes les mentions prévues par l'article 13 du RGPD.<br>L'information est au moins diffusée en commission ou en conférence médicale d'établissement, sur l'intranet de celui-ci et à l'aide d'affiches dans les lieux de repos des personnels.<br>En plus, la fiche d'information peut prendre la forme d'un courrier ou d'un courriel joint au bulletin de paie ou au contrat de travail. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de professionnels exerçant postérieurement à la constitution de l'entrepôt) | |
| **8.5.2** | Si l'entrepôt contient des données de professionnels n'exerçant pas ou plus au sein des établissements lors de la mise en œuvre de l'entrepôt, et que le responsable de traitement n'est pas l'employeur des professionnels : une information individuelle par écrit de chacun d'entre eux comprenant les mentions prévues à l'article 14 du RGPD est réalisée. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt ne contient pas de données de professionnels exerçant postérieurement à la constitution de l'entrepôt) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **9. Droits des personnes** | | | |
| **9.1** | Une information générale, à destination des professionnels de santé et des patients est réalisée par le responsable de traitement en complément de l'information individuelle et préalablement à la mise en place de l'entrepôt.[2]<br>Cette information générale s'effectue *via* une campagne d'information publique, par exemple sur les réseaux sociaux, au sein des établissements et par la publication d'encarts dans la presse régionale. | ☐ Vrai<br>☐ Faux | |
| **9.2** | Les professionnels et les patients peuvent exercer les droits suivants dans les conditions prévues par le RGPD :<br>• droit d'accès,<br>• droit de rectification,<br>• droit à l'effacement,<br>• droit à la limitation du traitement,<br>• droit d'opposition | ☐ Vrai<br>☐ Faux | |
| **9.4** | Le droit d'opposition du patient peut être exercé par tout moyen. Par ailleurs, les personnes peuvent s'opposer au traitement des données les concernant dans l'entrepôt dès leur information. | ☐ Vrai<br>☐ Faux | |
| **9.5** | Une personne spécifiquement formée et habilitée (par exemple, le DPO du responsable de traitement) s'assure de l'exercice des droits des personnes concernées. Ses coordonnées sont communiquées aux personnes concernées et figurent dans les différents supports d'information. | ☐ Vrai<br>☐ Faux | |
| **9.6** | Des mécanismes sont prévus pour garantir l'exercice des droits des personnes, lorsque les données identifiantes ou moyens de correspondance avec l'identité ne sont pas conservés.<br>Le responsable de traitement ne peut se prévaloir de l'article 11 RGPD pour écarter les demandes d'exercice des droits prévus par le RGPD. | ☐ Vrai<br>☐ Faux | |
| **9.7** | Des mécanismes d'alimentation de l'entrepôt permettent aux personnes d'exercer de façon pérenne leur droit d'opposition et peuvent constituer un moyen de réidentifier les données des personnes exerçant leurs autres droits. | ☐ Vrai<br>☐ Faux | |

[2] Cette campagne d'information générale a pour objectif de garantir qu'une période de temps raisonnable (par ex. : un mois) s'écoule entre la notification des patients et le commencement du traitement de leurs données, afin que ceux-ci puissent faire valoir leur droit d'opposition.

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **10. Sécurité – Cloisonnement réseau (« SEC-RES »)** | | | |
| **SEC-RES-1** | Des mesures de cloisonnement séparant les flux réseau spécifiques à l'entrepôt du reste des flux du système d'information ont été mises en place sur le réseau de communication au sein duquel l'entrepôt est hébergé ou rendu accessible. | ☐ Vrai<br>☐ Faux | |
| **SEC-RES-2** | Des mesures de filtrage sont mises en œuvre afin de restreindre l'émission et la réception de ces flux réseau aux seules machines spécifiquement identifiées et autorisées pour le fonctionnement de l'entrepôt. | ☐ Vrai<br>☐ Faux | |
| **SEC-RES-3** | Toutes les transmissions de données depuis ou vers l'entrepôt, ainsi que tous les flux de données internes à l'entrepôt, font l'objet de mesures de chiffrement conformes à l'annexe B1 du référentiel général de sécurité (« RGS ») afin d'en garantir la confidentialité. | ☐ Vrai<br>☐ Faux | |
| **10. Sécurité – Cloisonnement logique et cryptographique (« SEC-LOG »)** | | | |
| **SEC-LOG-1** | Les données personnelles faisant partie de l'entrepôt sont collectées ou stockées sur des systèmes et bases de données distincts de ceux assurant la prise en charge des patients. | ☐ Vrai<br>☐ Faux | |
| **SEC-LOG-2** | Les données personnelles sont chiffrées au repos par des algorithmes et tailles de clé conformes à l'annexe B1 du RGS, et une procédure opérationnelle de gestion des clés a été formalisée. | ☐ Vrai<br>☐ Faux | |
| **SEC-LOG-3** | Les sauvegardes de l'entrepôt font l'objet d'un chiffrement au repos conforme à l'annexe B1 du RGS. | ☐ Vrai<br>☐ Faux | |
| **SEC-LOG-4** | Dans le cas où des données directement identifiantes ou des tables de correspondance sont stockées dans l'entrepôt, celles-ci sont séparées logiquement des données pseudonymisées par des moyens cryptographiques.<br>Par exemple : les données administratives des patients et les tables de correspondance sont chiffrées avec des clés différentes de celles utilisées pour chiffrer les données de santé de l'entrepôt. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si des données directement identifiantes ou des tables de correspondance ne sont pas stockées) | |
| **SEC-LOG-5** | L'accès aux deux catégories de données séparées définies à l'exigence SEC-LOG-4 est effectué via des comptes utilisateur différents, ou via un seul compte utilisateur devant choisir à la connexion un des profils d'habilitation différents qui lui sont attribués. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'exigence SEC-LOG-4 n'est pas applicable) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **SEC-LOG-6.1** | Dans le cas où des données génétiques ou de suivi de localisation sont collectées, celles-ci font l'objet d'un chiffrement distinct avec une clé spécifique par rapport aux autres données de l'entrepôt. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si des données génétiques ou de suivi de localisation ne sont pas collectées) | |
| **SEC-LOG-6.2** | La clé de déchiffrement des données génétiques ou de suivi de localisation n'est mobilisable que par les profils d'habilitation responsables de l'alimentation de l'entrepôt et de l'exportation de données vers un espace de travail. | ☐ Vrai<br>☐ Faux | |
| **10. Sécurité – Constitution et alimentation de l'entrepôt (« SEC-ALI »)** | | | |
| **SEC-ALI-1** | Les circuits de collecte des données font l'objet de mesures de sécurité appropriées.<br>Par exemple : les répertoires de transit sont purgés régulièrement. Un contrôle d'accès strict aux données collectées est mis en place. | ☐ Vrai<br>☐ Faux | |
| **SEC-ALI-2** | Dans le cas où l'entrepôt est alimenté manuellement *via* des logiciels de saisie autorisant également la consultation des données saisies, les accès à ces logiciels sont sécurisés *via* une authentification forte conforme à l'exigence SEC-AUT-1. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si aucun logiciel de saisie de données patient n'est mis en place au sein de l'entrepôt) | |
| **10. Sécurité – Pseudonymisation des données (« SEC-PSE »)** | | | |
| **SEC-PSE-1.1** | Aucun numéro interne, tel qu'un numéro de dossier patient, n'est directement réutilisé comme identifiant au sein de l'entrepôt. | ☐ Vrai<br>☐ Faux | |
| **SEC-PSE-1.2** | Un identifiant pseudonyme unique est utilisé, permettant le cas échéant la correspondance entre les données pseudonymisées stockées dans l'entrepôt et des données directement identifiantes. | ☐ Vrai<br>☐ Faux | |
| **SEC-PSE-1.3** | Cet identifiant pseudonyme unique est dédié à un seul entrepôt et est généré par une fonction de hachage cryptographique résistante aux attaques par force brute ou un générateur de nombres pseudo-aléatoires cryptographiquement sûr. | ☐ Vrai<br>☐ Faux | |
| **SEC-PSE-1.4** | Les données sont pseudonymisées préalablement à leur intégration dans l'entrepôt. | ☐ Vrai<br>☐ Faux | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **SEC-PSE-2** | Dans le cas où l'entrepôt intègre des jeux de données existants déjà pseudonymisés, un nouveau numéro pseudonyme unique respectant les conditions de l'exigence SEC-PSE-1 est généré lors de l'alimentation de l'entrepôt. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si aucun jeu de données préexistant et déjà pseudonymisées n'est intégré à l'entrepôt) | |
| **SEC-PSE-3** | Dans le cas où des données relatives aux professionnels de santé sont collectées, ces données sont pseudonymisées. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si les données relatives aux professionnels de santé ne sont pas collectées) | |
| **SEC-PSE-4** | Dans le cas où des documents non structurés sont ajoutés à l'entrepôt, ceux-ci font l'objet d'une étape de suppression ou de masquage avant leur intégration dans l'entrepôt.<br>L'opération de masquage ou suppression est appliquée à la fois au contenu visible des documents (comme les entêtes des courriers et les cartouches des images), aux métadonnées contenues dans ces fichiers (comme le nom de l'opérateur d'imagerie) et aux attributs des fichiers (comme leur nom).<br>Cette étape consiste à supprimer les données identifiantes des patients et des professionnels de santé ou à les remplacer par des termes génériques ou des données fictives. Par exemple, les NIR, nom de naissance, prénom, code postal, ville ou numéro de téléphone seront remplacés par des termes génériques tels que « NIR », « NOM_DE_NAISSANCE », « PRENOM », « CODE_POSTAL », « VILLE » ou « TEL ».<br>Cette exigence s'applique notamment aux documents bureautiques et aux fac-similés d'impression (comme les comptes rendus médicaux et les prescriptions), aux numérisations de documents, à l'imagerie médicale et à toute forme de résultats d'analyse biomédicale. Elle concerne également les commentaires en saisie libres contenus dans les bases de données. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si aucun document non structuré n'est intégré à l'entrepôt) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **10. Sécurité – Accès physique aux données (« SEC-PHY »)** | | | |
| **SEC-PHY-1** | L'accès physique aux serveurs et aux locaux hébergeant les infrastructures de l'entrepôt est sécurisé par des mesures de protection adéquates ; en particulier, des mesures de contrôle d'accès physique. | ☐ Vrai<br>☐ Faux | |
| **10. Sécurité – Gestion des habilitations et accès logique aux données (« SEC-HAB »)** | | | |
| **SEC-HAB-1** | Différents profils d'habilitation sont prévus afin de gérer les accès aux données en tant que besoin et de façon exclusive. | ☐ Vrai<br>☐ Faux | |
| **SEC-HAB-2** | Une granularité des accès aux données est prévue pour chaque profil d'habilitation, tout en respectant l'exigence SEC-LOG-5 relative au cloisonnement des tables de correspondance et données directement identifiantes.<br>Par exemple : un profil peut contenir soit un accès uniquement à des données agrégées et/ou un accès à des données pseudonymisées, soit un accès uniquement à des données directement identifiantes. | ☐ Vrai<br>☐ Faux | |
| **SEC-HAB-3** | Les personnes autorisées à accéder aux données personnelles sont individuellement habilitées selon une procédure impliquant une validation par :<br>• une des instances assurant la gouvernance de l'entrepôt ; ou<br>• par leur responsable hiérarchique dans le cas des ingénieurs et administrateurs système et réseau. | ☐ Vrai<br>☐ Faux | |
| **SEC-HAB-4** | Les accès privilégiés disposant de droits étendus, notamment pour l'administration et la maintenance sont réservés à une équipe restreinte et limités au strict nécessaire. | ☐ Vrai<br>☐ Faux | |
| **SEC-HAB-5** | Une revue manuelle ou automatique des habilitations est réalisée régulièrement et au moins annuellement, ainsi qu'à la fin de chaque projet de recherche utilisant les données de l'entrepôt. | ☐ Vrai<br>☐ Faux | |
| **SEC-HAB-6** | Les permissions d'accès sont retirées dès le retrait des habilitations, par exemple après le départ d'un collaborateur ou une modification de ses missions. | ☐ Vrai<br>☐ Faux | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **10. Sécurité – Authentification pour la consultation et l'administration de l'entrepôt (« SEC-AUT »)** | | | |
| **SEC-AUT-1.1** | L'accès aux données personnelles est subordonné à une authentification forte (multifacteur) faisant intervenir au moins deux facteurs d'authentification distincts. | ☐ Vrai<br>☐ Faux | |
| **SEC-AUT-1.2** | Dans le cas où un de ces facteurs est un mot de passe, celui-ci est conforme aux recommandations de la CNIL en matière de mot de passe (délibération n° 2017-012 du 19 janvier 2017 à la date de rédaction de ce référentiel, ou toute autre mise à jour de cette recommandation). | ☐ Vrai<br>☐ Faux<br>☐ N/A (si aucun des facteurs d'authentification n'est un mot de passe) | |
| **SEC-AUT-2** | Cette authentification forte est mise en place à la fois pour les accès internes et externes à l'entrepôt. | ☐ Vrai<br>☐ Faux | |
| **SEC-AUT-3** | Toutes les transmissions de données depuis ou vers l'entrepôt, ainsi que tous les flux internes à l'entrepôt, réalisés automatiquement sans action d'un utilisateur, sont effectuées par des serveurs mutuellement authentifiés par certificat ou dispositif d'authentification équivalent.<br>Un mot de passe seul n'est pas considéré comme un dispositif d'authentification équivalent à un certificat. | ☐ Vrai<br>☐ Faux | |
| **10. Sécurité – Espace de travail (« SEC-ESP »)** | | | |
| **SEC-ESP-1** | Les données de l'entrepôt sont manipulées par les chercheurs uniquement dans des espaces de travail internes à l'entrepôt et spécifiques à chaque projet de recherche, étanches avec la base de données de l'entrepôt et étanches les uns des autres.(Seuls des capacités d'échange entre les espaces de travail sont possibles pour le partage de données qui auront subi le processus d'anonymisation détaillé à l'exigence SEC-EXP-1.) | ☐ Vrai<br>☐ Faux | |
| **SEC-ESP-2.1** | Les jeux de données importées dans un espace de travail spécifique à un projet de recherche sont minimisés et limités aux seules données nécessaires au projet. | ☐ Vrai<br>☐ Faux | |
| **SEC-ESP-2.2 et SEC-ESP-3** | Un numéro pseudonyme unique spécifique à chaque espace de travail est généré dans les mêmes conditions qu'à l'exigence SEC-PSE-1. (En cas de suivi de cohorte, le même numéro pseudonyme unique peut être réutilisé dans plusieurs espaces de travail.) | ☐ Vrai<br>☐ Faux | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **10. Sécurité – Exportation de données hors de l'entrepôt et hors des espaces de travail (« SEC-EXP »)** | | | |
| **SEC-EXP-1** | À l'exception des données relatives aux procédures de ré-identification SEC-REI-1 à SEC-REI-3, seuls des jeux de données anonymes font l'objet d'une exportation hors de l'entrepôt ou d'un espace de travail.<br>Le processus d'anonymisation produit un jeu de données conforme aux trois critères définis par l'avis du G29 n° 05/2014 ou à tout avis ultérieur du CEPD relatif à l'anonymisation. Cette conformité est documentée et démontrable.<br>À défaut, si ces trois critères ne peuvent être réunis, une étude des risques de ré-identification est menée et documentée. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt n'inclut pas de fonctionnalité d'exportation de données) | |
| **SEC-EXP-2** | Les exports de données sont soumis à la validation préalable d'un responsable afin d'en avaliser le principe, notamment au regard de l'exigence SEC-EXP-1. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt n'inclut pas de fonctionnalité d'exportation de données) | |
| **SEC-EXP-3.1** | Les exports font l'objet d'une surveillance automatique ou manuelle par un opérateur spécialisé afin d'en vérifier le caractère anonyme. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si l'entrepôt n'inclut pas de fonctionnalité d'exportation de données) | |
| **SEC-EXP-3.2** | Dans le cas où cette surveillance est automatique, tout export identifié comme non conforme fait l'objet d'une remontée d'alerte et d'une mise en quarantaine dans l'entrepôt, puis est vérifié manuellement par un responsable spécifiquement formé et spécifiquement habilité. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si la surveillance des exports est manuelle) | |
| **SEC-EXP-4** | Les systèmes mis en place dans l'entrepôt relatifs à la production d'indicateurs et au pilotage stratégique de l'activité d'un établissement de santé ne permettent que des restitutions anonymes, y compris en tenant compte des fonctionnalités de filtrage et de sélection de ces restitutions.<br>Ce processus de restitution est conforme aux trois critères définis par l'avis du G29 n° 05/2014 ou à tout avis ultérieur du CEPD | ☐ Vrai<br>☐ Faux<br>☐ N/A (si la finalité de l'entrepôt ne comprend pas la production d'indicateurs et le pilotage stratégique de l'activité d'un | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| | relatif à l'anonymisation. Cette conformité est documentée et démontrable.<br>À défaut, si ces trois critères ne peuvent être réunis, une étude des risques de ré-identification est menée et documentée. | établissement de santé) | |
| **SEC-EXP-5** | Les restitutions mentionnées à l'exigence SEC-EXP-4 sont exportées conformément aux exigences SEC-EXP-2 et SEC-EXP-3. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si la finalité de l'entrepôt ne comprend pas la production d'indicateurs et le pilotage stratégique de l'activité d'un établissement de santé) | |
| **10. Sécurité – Sensibilisation des utilisateurs et sécurité des postes de travail (« SEC-SEN »)** | | | |
| **SEC-SEN-1** | Chaque personne habilitée à accéder à l'entrepôt est formée au respect du secret médical et sensibilisée régulièrement aux risques et obligations inhérents au traitement de données de santé. | ☐ Vrai<br>☐ Faux | |
| **SEC-SEN-2** | Chaque personne habilitée à accéder à l'entrepôt signe une charte de confidentialité précisant notamment ses obligations au regard de la protection des données personnelles de santé et au regard des mesures de sécurité mises en place dans l'entrepôt, ainsi que les sanctions afférentes au non-respect de ces obligations. | ☐ Vrai<br>☐ Faux | |
| **SEC-SEN-3.1** | Les postes de travail des personnes habilitées à accéder à l'entrepôt y compris les utilisateurs externes accédant uniquement aux espaces de travail, font l'objet de mesures de sécurité spécifiques, par exemple en mettant en place des comptes nominatifs, une authentification adéquate, un verrouillage automatique des sessions, un chiffrement des supports de stockage et des mesures de filtrage. | ☐ Vrai<br>☐ Faux | |
| **SEC-SEN-3.2** | Dans le cas où les postes de travail ne sont pas sous le contrôle du responsable de traitement, les mesures de sécurité à mettre en place sur les postes de travail sont encadrées au moyen d'une convention entre les parties concernées. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si les postes de travail sont sous le contrôle du responsable de traitement) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **10. Sécurité – Journalisation (« SEC-JOU »)** | | | |
| **SEC-JOU-1** | Les actions des utilisateurs des espaces de travail de l'entrepôt font l'objet de mesures de journalisation. En particulier, les connexions à l'entrepôt (identifiants, date et heure), les requêtes et opérations réalisées sont tracées. | ☐ Vrai<br>☐ Faux | |
| **SEC-JOU-2** | Les accès des ingénieurs et administrateurs système et réseau sont effectués à travers un système spécifique assurant une authentification forte ainsi que la traçabilité détaillée des accès et actions réalisés. (Par exemple, un bastion d'administration peut être utilisé pour contrôler les accès et enregistrer les sessions.) | ☐ Vrai<br>☐ Faux | |
| **SEC –JOU-3** | Un contrôle des traces est réalisé régulièrement et au moins bimestriellement, ainsi qu'à la fin de chaque période d'habilitation liée à un projet de recherche. Ce contrôle est réalisé par :<br>• une solution réalisant une surveillance automatique avec une remontée d'alertes traitées manuellement par un opérateur habilité ;<br>• ou par un contrôle semi-automatique *via* exécution de programmes permettant une sélection des traces anormales, suivi d'une relecture manuelle par un opérateur habilité. | ☐ Vrai<br>☐ Faux | |
| **SEC-JOU-4** | Les traces de journalisation définies aux exigences SEC-JOU-1 et SEC-JOU-2 sont conservées pendant une durée de comprise entre 6 mois et un an. | ☐ Vrai<br>☐ Faux | |
| **10. Sécurité – Procédures de ré-identification (« SEC-REI »)** | | | |
| **SEC-REI-1** | Le responsable de traitement a mis en place une procédure opérationnelle sécurisée afin d'assurer l'exercice des droits des personnes et le cas échéant la levée du pseudonymat et la bonne ré-identification des personnes concernées.<br>Cette procédure permet, à partir des informations supplémentaires nécessaires à l'identification unique de la personne, de retrouver ou de calculer le numéro pseudonyme unique correspondant, puis de sélectionner dans l'entrepôt, avec ce seul numéro pseudonyme unique, les données correspondant au demandeur et d'effectuer les opérations nécessaires au bon exercice de ses droits (suppression des données ou extraction pour transmission). | ☐ Vrai<br>☐ Faux<br>☐ N/A (s'il n'est pas prévu de mécanisme de levée du pseudonymat) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **SEC-REI-2** | Le cas échéant, et en cas de nécessité dûment justifiée et documentée, le responsable de traitement a mis en place une procédure opérationnelle sécurisée afin de recontacter des patients pour leur proposer de participer à des recherches.<br>Cette procédure permet, à partir d'une liste de critères médicaux, de sélectionner les identifiants pseudonymes uniques correspondants aux patients visés, puis, en mobilisant la ou les tables de correspondance de l'entrepôt avec ces seuls pseudonymes, de sélectionner les données identifiantes correspondant à ces patients afin de les exporter pour cette seule finalité. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si aucune ré-identification pour participation à une recherche n'est possible) | |
| **SEC-REI-3** | Le cas échéant, le responsable de traitement a mis en place une procédure opérationnelle sécurisée afin de ré-identifier des patients en cas d'urgence médicale.<br>Cette procédure permet, en mobilisant la ou les tables de correspondance de l'entrepôt, de sélectionner les données identifiantes des patients concernés à partir de leur numéro pseudonyme unique, et de les exporter pour cette seule finalité. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si aucune ré-identification pour urgence médicale n'est possible) | |
| **SEC-REI-4** | Les habilitations et accès relatifs aux procédures de ré-identification définies aux exigences SEC-REI-1 à SEC-REI-3 sont uniquement réservés à une équipe restreinte et limités au strict nécessaire.Les membres de cette équipe restreinte sont formés spécifiquement à cette procédure. | ☐ Vrai<br>☐ Faux | |
| **SEC-REI-5** | Le responsable de traitement a mis en œuvre les mesures adéquates pour gérer les risques inhérents à ces procédures de ré-identification et notamment pour garantir qu'elles ne soient utilisables que dans le cas d'une demande émanant effectivement d'une personne concernée ou d'un professionnel de santé dûment habilité. | ☐ Vrai<br>☐ Faux | |
| **10. Sécurité – Gestion des incidents de sécurité et des violations de données personnelles (« SEC-INC »)** | | | |
| **SEC-INC-1** | Le responsable de traitement a mis en place une procédure de gestion et de traitement des incidents de sécurité et des violations de données personnelles, précisant les rôles et responsabilités et les actions à mener en cas de survenue de tels incidents. | ☐ Vrai<br>☐ Faux | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| SEC-INC-2 | Tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence, même temporaire, de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles, fait l'objet d'une documentation en interne dans un registre des violations. | ☐ Vrai<br>☐ Faux | |
| SEC-INC-3 | Lorsqu'un tel incident est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées, la violation de données qui en résulte est notifiée à la Commission dans les conditions prévues à l'article 33 du RGPD. | ☐ Vrai<br>☐ Faux | |
| SEC-INC-4 | Dans l'hypothèse où la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable de traitement communique la violation des données aux personnes concernées dans les meilleurs délais, conformément à l'article 34 du RGPD. | ☐ Vrai<br>☐ Faux | |
| **11. Sous-traitants** | | | |
| 11.1 | En cas de recours à un prestataire : un contrat est conclu avec celui-ci conformément aux dispositions de l'article 28 RGPD. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si le responsable de traitement n'a pas recours à un sous-traitant) | |
| 11.1 | La répartition des responsabilités en matière de sécurité et de gestion des violations de données entre le responsable de l'entrepôt et le prestataire est prévue par le contrat. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si le responsable de traitement n'a pas recours à un sous-traitant) | |
| 11.2 | Le prestataire tient un registre des activités de traitement dans les conditions posées à l'article 30.2 RGPD. | ☐ Vrai<br>☐ Faux<br>☐ N/A (si le responsable de traitement n'a pas recours à un sous-traitant) | |

| Point du référentiel | Critères | Réponse | Raison de la non-conformité |
|---|---|---|---|
| **11.3** | Le sous-traitant auquel l'entrepôt a recours relève exclusivement des juridictions de l'Union européennes ou d'un pays considéré comme adéquat au sens de l'article 45 du RGPD.[3] | ☐ Vrai<br>☐ Faux<br>☐ N/A<br>(si le responsable de traitement n'a pas recours à un sous-traitant) | |
| **11.4** | Si le sous-traitant est recruté pour l'hébergement, le stockage ou la conservation des données : il est agréé ou certifié hébergeur de données de santé selon les dispositions du code de la santé publique. | ☐ Vrai<br>☐ Faux<br>☐ N/A<br>(si le responsable de traitement n'a pas recours à un sous-traitant) | |
| **12. Transferts de données hors de l'Union européenne** | | | |
| **12.2** | La mise en place et le fonctionnement de l'entrepôt n'entraînent pas le transfert de données personnelles, directement ou indirectement identifiantes, hors de l'Union européenne ou à destination d'un pays ne disposant pas d'un niveau de protection adéquat. | ☐ Vrai<br>☐ Faux | |
| **13. Analyse d'impact sur la protection des données (AIPD)** | | | |
| **13.1** | Une analyse d'impact sur la protection des données complète et répondant aux exigences de l'article 35 du RGPD a été réalisée. | ☐ Vrai<br>☐ Faux | |
| **13.4** | L'analyse d'impact est réexaminée et mise à jour régulièrement, notamment en cas de changement substantiel intervenant dans le traitement ou en cas de nouveaux risques pour les personnes concernées. | ☐ Vrai<br>☐ Faux | |

[3] Pour plus d'informations sur les pays considérés comme adéquats, voir la carte de la protection des données dans le monde sur cnil.fr.