Attention, cette liste d'exigences réglementaire date d'avril 2024. Elle n'aura pas été mise à jour au moment où vous consulterez ce document.

La nouvelle application de collecte France Cohortes prendra en charge des cohortes de type "clinique" parmi lesquelles:
1) certaines sont conformes avec une méthodologie de référence (MR-001, MR-003, MR-004) nécessitant uniquement réaliser une déclaration de conformité auprès de la CNIL ;
2) d'autres ne rentrent pas dans le cadre des MR et font l'objet d'une demande d'autorisation CNIL.
3) d'autres souhaitent la collecte d'une grande quantité de données pour alimenter une base de données et les réutiliser dans des études ultérieures, ce qui fera l'objet d'une déclaration de conformité au référentiel sur les EDS.

Cas n°1 : Pour pouvoir prendre en charge les cohortes concernées par les MR, il est nécessaire que l'application remplisse les obligations présentes dans les méthodologies de référence de la CNIL.

Cas n°2 : La CNIL explique dans sa publication "Traitements de données de santé : comment faire la distinction entre un entrepôt et une recherche et quelles conséquences ?" du 02 mars 2023 que :
"Les cohortes prévoyant un suivi longitudinal, dans une durée limitée, portant sur une thématique précise et ayant des destinataires limités sont des recherches et relèvent des dispositions spécifiques qui leur sont applicables".
Toutefois, certaines des cohortes prises en charge par France Cohortes ne correspondront pas à cette description (collecte des catégories de données hors du périmètre des MR, objectif de recherche large, durée supérieure à 10 ans) et devront donc faire une demande d'autorisation spécifique auprès de la CNIL.

Cas n° 3 : Il est aussi possible que certaines cohortes visent à collecter des données pour alimenter un EDS et les utiliser ultérieurement ; dans ce cas, elles relèveront du régime des EDS et du référentiel de sécurité associé.
A noter que le référentiel EDS comprend des dispositions de sécurité applicables à des catégories de données qui ne sont pas comprises par les MR (données génétiques) et souvent collectées par les cohortes, dont la mise en œuvre protègera mieux les droits des personnes que les seules obligations présentes dans les MR.

Pour s'assurer que l'outil mis en place puisse prendre en charge indifféremment ces différentes cohortes, nous avons donc listé ici les exigences réglementaires provenant des sources suivantes:
- le référentiel des EDS de la CNIL
- les méthodologies de référence de la CNIL
- les règles de sécurité standards présentes dans les guides de sécurité et des articles publiées par la CNIL ou l'ANSSI (bonnes pratiques)

Cette démarche s'aligne par ailleurs avec l'objectif de la CNIL qui vise à faire que le travail de recherche sur des données se fasse dans des espaces sécurisées type EDS (voir extrait du CR de l'"Atelier CNIL n°2 – Entrepôt de données de Santé" : "l'idée est qu'à terme les EDS soient la seule source d'accès à des données pour la recherche avec des espaces de travail sécurisés, et que cela soit pratique pour les chercheurs").
Les autres exigences indépendantes de l'outil (comme réaliser une analyse d'impact) ne seront pas listées ici car décorrélées du choix de l'outil.

Sources :
Publication sur les EDS de la CNIL : https://www.cnil.fr/fr/traitements-de-donnees-de-sante-comment-faire-la-distinction-entre-un-entrepot-et-une-recherche-et
Référentiel EDS : https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_entrepot.pdf
Atelier EDS : https://www.chu-hugo.fr/accueil/wp-content/uploads/sites/2/2020/06/20221012-CR-Atelier-2-CNIL_CRv1.0-1.pdf
MR 001 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037187386
MR 002 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031074605
MR 003 : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037187443
MR 004: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037187498
CNIL "sécuriser son site web": https://www.cnil.fr/fr/securite-securiser-les-sites-web
Guide ANSSI : https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/
Guide CNIL sécurité : https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_guide_securite_personnelle.pdf

Liste des écarts au référentiel :
- gestion de l'identifiant patient sous format XXX-YYY-AB (avec XXX: numéro du centre dans la cohorte, YYY: numéro du patient dans le centre et AB: initiales du patient) au lieu d'un identifiant pseudonyme unique généré par une fonction de hachage cryptographique (SEC-PSE-1)
- la mise en place d'un outil de contrôle automatique des logs (SEC-JOU-3)
- Gestion des données génétiques et localisation semble complexe à mettre en place (aucun logiciel du marché ne prévoit un type de donnée à part pour génétique/localisation)

N°	Nom	Importance	Type	Source	Extrait du texte	Description du besoin / Analyse
ER-1	Exigence de sécurité SEC-LOG-1	**Critique**	**Données identifiantes**	Référentiel des EDS de la CNIL	*"Le responsable de traitement doit collecter et stocker les données à caractère personnel faisant partie de l'entrepôt sur des systèmes et bases de données distincts de ceux assurant la prise en charge des patients."*	Les bases de donneés de l'outil de collecte lui seront dédiés donc pas d'impact important. Si "on premise" : héberger la base de données applicative sur une VM dédiée Saas : disposer de VM dédiées à l'usage de France Cohortes
ER-2	Exigence de sécurité SEC-LOG-2	**Critique**	**Données identifiantes**	Référentiel des EDS de la CNIL	*"Les données à caractère personnel doivent être chiffrées au repos par des algorithmes et tailles de clé conformes à l'annexe B1 du RGS. Une procédure opérationnelle de gestion des clés doit être formalisée."*	Les **données à caractère personnel doivent être chiffrées au repos** dans l'application (conforme annexe B1 RGS). Cette gestion des clés doit être géré par l'outil
ER-3	Exigence de sécurité SEC-LOG-3	**Critique**	**Données identifiantes**	Référentiel des EDS de la CNIL	*"Les sauvegardes de ces données doivent également faire l'objet d'un chiffrement conforme à l'annexe B1 du RGS."*	Les **sauvegardes des données (personnelles) doivent être chiffrées** (conforme annexe B1 RGS)

ER-4	Exigence de sécurité SEC-LOG-4	**Critique**	**Données identifiantes**	Référentiel des EDS de la CNIL	*"Dans le cas où des données directement identifiantes ou des tables de correspondance sont stockées dans l'entrepôt, celles-ci doivent être séparées logiquement des données pseudonymisées par des moyens cryptographiques. Par exemple, les données administratives des patients et les tables de correspondance doivent être chiffrées avec des clés différentes de celles utilisées pour chiffrer les données de santé de l'entrepôt"*	Les **données identifiantes** doivent être stockées **dans une base séparée** des autres données.
ER-5	Exigence de sécurité SEC-LOG-5	**Hors scope**	**Données identifiantes**	Référentiel des EDS de la CNIL	*"L'accès aux deux catégories de données séparées définies à l'exigence SEC-LOG-4 doit être 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."*	Le fait que les personnels aient déjà besoin d'un profil pour accéder aux études suffit à priori? (à confirmer)
ER-6	Exigence de sécurité SEC-LOG-6	**Faible**	**Données identifiantes**	Référentiel des EDS de la CNIL	*"Dans le cas où des données génétiques ou de suivi de localisation sont collectées, celles-ci doivent faire l'objet d'un chiffrement distinct avec une clé spécifique par rapport aux autres données de l'entrepôt.* *La clé de déchiffrement des données génétiques ou de suivi de localisation ne doit être 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."*	Les données de génétique et de localisation doivent être chifrées **différemment** des autres données identifiantes. A vérifier ce que données génétiques veut dire : nous n'aurons pas de séquençage dans l'application mais des résultats. A ma connaissance aucun outil ne gère une catégorie de données "génétiques", cela risque donc de poser problème si nous sommes soumis à cette obligation.
ER-7	Limitation de l'accès aux données	**Critique**	**Données identifiantes**	Référentiel des EDS de la CNIL	*"6.2 : L'accès et l'usage des données directement identifiantes doivent être 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."*	L'outil doit **permettre de restreindre l'accès aux données identifiantes à des catégories de personnes identifiées** (droit de modification et droit de vision des variables identifiantes en fonction du profil d'accès de la personne).
ER-8	Conservation des données	**Critique**	**Conservation des données**	Référentiel des EDS de la CNIL	*"7.2 : Les données mentionnées au point 5.2.1.2 peuvent être conservées 20 ans maximum à compter de leur collecte dans le cadre des soins ou des recherches. Les données mentionnées au point 5.2.1.1 doivent être supprimées lorsque le délai de conservation des données mentionnées au point 5.2.1.2 a expiré.* *7.3: Au-delà de ces durées, toute donnée doit être anonymisée ou détruite.* *9.2: Les personnes concernées (professionnels et patients) dont les données figurent dans l'entrepôt disposent des droits suivants, qu'elles exercent dans les conditions prévues par le RGPD :* *- droit d'accès ;* *- droit de rectification ;* *- droit à l'effacement ;* *- droit à la limitation du traitement ;"*	Pour la durée de conservation: Si les données sont conservées durablement dans l'outil alors un traitement manuel par FC pourrait être mis en place afin de **supprimer les cohortes dont la durée de conservation excède les dispositions de la CNIL**. Sinon si les données sont conservées dans un espace de stockage alors on pourra supprimer les données collectées de l'outil après export (en supprimant le projet par exemple). Pour les droits du RGPD: L'outil devra permettre de supprimer les données d'une personne ou d'une cohorte, ou de modifier les données saisies.
ER-9	Exigence de sécurité SEC-RES-1	**Critique**	**Réseau**	Référentiel des EDS de la CNIL	*"Le réseau de communication sur lequel l'entrepôt est hébergé ou rendu accessible doit faire l'objet de mesures de cloisonnement séparant les flux réseau spécifiques à l'entrepôt du reste des flux du système d'information."*	Le cloisonnement réseau réduit les impacts en cas de compromission. On peut distinguer un réseau interne sur lequel aucune connexion venant d'Internet n'est autorisée, et un réseau DMZ (DeMilita- rized Zone) accessible depuis Internet, en les séparant par des passerelles (« gateway »). À ce sujet, l'ANSSI a publié des recommandations relatives à l'interconnexion d'un système d'information à Internet, En bref : utilisation des bonnes pratiques réseau : **pare-feu, DMZ...** L'outil étant à destination de personnel externe et de patients de la cohorte, le portail de connexion devra être disponible sur internet (en DMZ si "on premise"). https://www.cnil.fr/fr/securite-proteger-le-reseau-informatique-interne
ER-10	Exigence de sécurité SEC-RES-2	**Critique**	**Réseau**	Référentiel des EDS de la CNIL	*"Des mesures de filtrage doivent également restreindre l'émission et la réception de ces flux réseau aux machines spécifiquement identifiées et autorisées pour le fonctionnement de l'entrepôt."*	Utilisation du **HTTPS avec TLS 1.3 + filtrer les flux entrants/sortants** sur les équipements (ex : pare-feux, serveurs proxy et autres). Par exemple, il faut autoriser uniquement les flux entrants sur cette machine sur le port 443 et bloquer tous les autres ports **(matrice de flux)** **Restreindre l'accès direct aux VM à une liste d'IP arrêtée et en SSH (pas de Telnet)** **Test d'intrusion et tests automatiques de vulnérabilité** https://www.cnil.fr/fr/securite-proteger-le-reseau-informatique-interne

ER-11	Exigence de sécurité SEC-RES-3	**Critique**	**Réseau**	Référentiel des EDS de la CNIL	*"Toutes les transmissions de données depuis ou vers l'entrepôt, ainsi que tous les flux de données internes à l'entrepôt, doivent faire l'objet de mesures de chiffrement conformes à l'annexe B1 du référentiel général de sécurité (« RGS ») afin d'en garantir la confidentialité."*	Les **flux de données sont chiffrées selon une méthode conforme à l'annexe B1 du référentiel RGS** https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf Par exemple : AES 128 bits
ER-12	Exigence de sécurité SEC-ALI-1	**Critique**	**Authentification et contrôle d'accès**	Référentiel des EDS de la CNIL	*"Les circuits de collecte des données doivent faire l'objet de mesures de sécurité appropriées, en particulier la purge régulière des répertoires de transit et un contrôle d'accès strict aux données collectées"*	Il n'y aura pas de répertoire de transit. Il faut un contrôle strict d'accès aux données : l'outil doit **permettre une gestion des droits à granularité fine (restriction d'accès aux données par centre, en fonction du profil attribué sur la cohorte…)**
ER-13	Exigence de sécurité SEC-ALI-2	**Critique**	**Authentification et contrôle d'accès**	Référentiel des EDS de la CNIL	"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 doivent être sécurisés via une authentification forte conforme à l'exigence SEC-AUT-1."	**Authentification forte pour les professionnels qui auront accès à l'outil de collecte.**
ER-14	Exigence de sécurité SEC-PSE-1	**Majeure**	**Pseudonymisation**	Référentiel des EDS de la CNIL	*"Aucun numéro interne, tel qu'un numéro de dossier patient ne peut être directement réutilisé comme identifiant au sein de l'entrepôt. Seul un identifiant pseudonyme unique peut être utilisé, permettant le cas échéant la correspondance entre les données pseudonymisées stockées dans l'entrepôt et des données directement identifiantes. Cet identifiant doit être dédié à un seul entrepôt. Il doit être généré par une fonction de hachage cryptographique résistante aux attaques par force brute ou un générateur de nombres pseudo-aléatoires cryptographiquement sûr. Les données doivent être pseudonymisées préalablement à leur intégration dans l'entrepôt."*	L'identifiant utilisé en général par les outils d'eCRF est sous la forme XXX-YYY-AB avec XXX = numéro du centre dans le projet, YYY = numéro du patient dans le centre et AB = initiales du patient (suivant les recommandations des méthodologies de référence : "*Lorsque le code alphanumérique se compose de lettres correspondant aux nom et prénom des personnes se prêtant à la recherche, il peut correspondre aux deux premières lettres du nom et à la première lettre du prénom. Il est toutefois recommandé de se limiter aux seules initiales, c'est-à-dire à la première lettre du nom et à la première lettre du prénom. Ces initiales peuvent être complétées d'un numéro d'inclusion et/ou d'un numéro de centre participant* "
ER-15	Exigence de sécurité SEC-PSE-2	**Hors scope**	**Pseudonymisation**	Référentiel des EDS de la CNIL	*"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 doit être généré lors de l'alimentation de l'entrepôt."*	N/A (pas d'alimentation avec des jeux de données existantes)
ER-16	Exigence de sécurité SEC-PSE-3	**Hors scope**	**Pseudonymisation**	Référentiel des EDS de la CNIL	*"Dans le cas où des données relatives aux professionnels de santé sont collectées, le responsable de traitement doit pseudonymiser ces données."*	Pas de donnée collectée sur les professionnels de santé en dehors des informations relatives à la création du compte (Nom/Prénom/Mail/Etablissement d'appartenance)
ER-17	Exigence de sécurité SEC-PSE-4	**Faible**	**Pseudonymisation**	Référentiel des EDS de la CNIL	*"Les documents non structurés ajoutés à l'entrepôt doivent faire l'objet d'une étape de suppression ou de masquage avant leur intégration dans l'entrepôt. 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 ».* *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.* *L'opération de masquage ou suppression devra s'appliquer 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)."*	Dans le cas de l'intégration de données non structurées dans l'outil de collecte (par exemple : champ d'upload DICOM au sein d'un formulaire), il faudra soit que **l'outil permette de masquer/supprimer les données identifiantes des patients/professionnels automatiquement soit que cela soit fait en amont de l'upload**
ER-18	Exigence de sécurité SEC-PHY-1	**Hors scope**	**Accès physique aux données**	Référentiel des EDS de la CNIL	*"L'accès physique aux serveurs et aux locaux hébergeant les infrastructures de l'entrepôt doit être sécurisé par des mesures de protection adéquates. En particulier, des mesures de contrôle d'accès physique doivent être mises en place."*	Obligation relevant du datacenter/hébergeur
ER-19	Exigence de sécurité SEC-HAB-1	**Faible**	**Accès logique aux données**	Référentiel des EDS de la CNIL	*"Différents profils d'habilitation doivent être prévus afin de gérer les accès aux données en tant que besoin et de façon exclusive."*	Obligation satisfaite par une gestion des profils avec des droits à granularité fine.
ER-20	Exigence de sécurité SEC-HAB-2	**Majeure**	**Accès logique aux données**	Référentiel des EDS de la CNIL	*"Une granularité des accès aux données doit être 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. 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."*	Voir SEC-LOG-5 et nécessité de créer un accès uniquement pour voir les données personnelles

ER-21	Exigence de sécurité SEC-HAB-3	**Hors scope**	**Accès logique aux données**	Référentiel des EDS de la CNIL	*"Les personnes autorisées à accéder aux données à caractère personnel doivent être individuellement habilitées selon une procédure impliquant une validation par : - une des instances assurant la gouvernance de l'entrepôt ; ou - par leur responsable hiérarchique dans le cas des ingénieurs et administrateurs système et réseau"*	Pas d'impact pour l'outil
ER-22	Exigence de sécurité SEC-HAB-4	**Hors scope**	**Accès logique aux données**	Référentiel des EDS de la CNIL	*"Les accès privilégiés disposant de droits étendus, notamment pour l'administration et la maintenance doivent être réservés à une équipe restreinte et être limités au strict nécessaire."*	Pas d'impact pour l'outil
ER-23	Exigence de sécurité SEC-HAB-5	**Faible**	**Accès logique aux données**	Référentiel des EDS de la CNIL	*"Une revue manuelle ou automatique des habilitations doit être réalisée régulièrement et a minima annuellement, ainsi qu'à la fin de chaque projet de recherche utilisant les données de l'entrepôt."*	Mettre en place un processus de désactivation des comptes utilisateur et faire une revue annuelle des comptes (notamment profils étendus). **<u>L'outil doit permettre de retirer l'habilitation d'un profil.</u>**
ER-24	Exigence de sécurité SEC-HAB-6	**Hors scope**	**Accès logique aux données**	Référentiel des EDS de la CNIL	*"Les permissions d'accès doivent être retirées dès le retrait des habilitations, par exemple après le départ d'un collaborateur ou une modification de ses missions"*	Pas d'impact pour l'outil
ER-25	Exigence de sécurité SEC-AUT-1	**Critique**	**Authentification et contrôle d'accès**	Référentiel des EDS de la CNIL	*"L'accès aux données à caractère personnel doit être subordonné à une authentification forte faisant intervenir a minima deux facteurs d'authentification distincts. Si un de ces facteurs est un mot de passe, celui-ci doit être 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)."*	**<u>Double authentification pour les professionnels accédant aux données personnelles et mot de passe respectant les recommandations de la CNIL et de l'ANSSI</u>** - la taille du mot de passe doit être au minimum de **12 caractères** ; et - le mot de passe doit comprendre des **majuscules, des minuscules, des chiffres et des caractères spéciaux.** ou - les mots de passe doivent être composés d'au minimum 1**4 caractères comprenant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire.** l'authentification doit faire intervenir une r**estriction de l'accès au compte**, qui doit prendre une ou plusieurs des formes suivantes : - une temporisation d'accès au compte après plusieurs échecs, dont la durée augmente exponentiellement dans le temps ; la commission recommande que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives par 24 heures ; et/ou - un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (p. ex. : « captcha ») ; et/ou - un blocage du compte après un nombre d'authentifications échouées consécutives au plus égal à 10.
ER-26	Exigence de sécurité SEC-AUT-2	**Hors scope**	**Authentification et contrôle d'accès**	Référentiel des EDS de la CNIL	*"Cette authentification forte doit être mise en place à la fois pour les accès internes et externes à l'entrepôt."*	Il n'y aura pas de différenciation entre accès interne et externe
ER-27	Exigence de sécurité SEC-AUT-3	**Faible**	**Authentification et contrôle d'accès**	Référentiel des EDS de la CNIL	*"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, doivent être effectués par des serveurs mutuellement authentifiés par certificat ou dispositif d'authentification équivalent"*	En cas de mise en place d'une transmission de données automatique (via l'API par exemple), il sera nécessaire que cette **<u>API soit sécurisée</u>** et permette d'authentifier les serveurs (via un token oAuth2 par exemple)
ER-28	Exigence de sécurité SEC-ESP-1	**Hors scope**	**Espace de travail**	Référentiel des EDS de la CNIL	*"Les données de l'entrepôt doivent être 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. Des capacités d'échange entre les espaces de travail sont néanmoins possibles pour le partage de données qui auront subi le processus d'anonymisation détaillé à l'exigence SEC-EXP-1"*	Les données seront manipulées dans les bulles sécurisées du SI France cohortes Pour des profesionnels appartenant à plusieurs cohortes, il ne faudra pas qu'ils travaillent sur les données de deux cohortes en même temps.
ER-29	Exigence de sécurité SEC-ESP-2	**Hors scope**	**Espace de travail**	Référentiel des EDS de la CNIL	*"Les jeux de données importées dans un espace de travail spécifique à un projet de recherche doivent être minimisés et limités aux seules données nécessaires au projet. Un numéro pseudonyme unique spécifique à chaque espace de travail devra être généré dans les mêmes conditions qu'à l'exigence SEC-PSE-1."*	Les jeux de données importés depuis l'outil de collecte seront limités aux seules données de la cohorte (soit des données nécessaires au projet)
ER-30	Exigence de sécurité SEC-ESP-3	**Hors scope**	**Espace de travail**	Référentiel des EDS de la CNIL	*"En cas de suivi de cohorte, le même numéro pseudonyme unique peut être réutilisé dans plusieurs espaces de travail"*	Pas d'impact pour l'outil
ER-31	Exigence de sécurité SEC-EXP-1	**Critique**	**Exportation de données**	Référentiel des EDS de la CNIL	*"A l'exception des données relatives aux procédures de ré-identification SEC-REI-1 à SEC-REI-3, seuls des jeux de données anonymes peuvent faire l'objet d'une exportation hors de l'entrepôt ou d'un espace de travail. Le processus d'anonymisation doit produire 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 doit être documentée et démontrable. À défaut, si ces trois critères ne peuvent être réunis, une étude des risques de ré-identification devra être menée et documentée."*	L'outil doit permettre de bloquer l'export des données identifiantes hors de l'outil

ER-32	Exigence de sécurité SEC-EXP-2	**Majeure**	**Exportation de données**	Référentiel des EDS de la CNIL	*"Les exports de données doivent être soumis à la validation préalable d'un responsable afin d'en avaliser le principe, notamment au regard de l'exigence SEC-EXP-1"*	L'outil doit permettre de limiter l'export à des profils autorisés
ER-33	Exigence de sécurité SEC-EXP-3	**Critique**	**Exportation de données**	Référentiel des EDS de la CNIL	*"Les exports doivent faire l'objet d'une surveillance automatique ou manuelle par un opérateur spécialisé afin d'en vérifier le caractère anonyme. Dans le cas où cette surveillance est automatique, tout export identifié comme non conforme doit faire l'objet d'une remontée d'alerte et d'une mise en quarantaine dans l'entrepôt, puis doit être vérifié manuellement par un responsable spécifiquement formé et spécifiquement habilité"*	L'outil doit permettre de bloquer l'export des données identifiantes hors de l'outil (sauf exception via un process spécifique)
ER-34	Exigence de sécurité SEC-EXP-4	**Hors scope**	**Exportation de données**	Référentiel des EDS de la CNIL	*"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 doivent permettre que des restitutions anonymes, y compris en tenant compte des fonctionnalités de filtrage et de sélection de ces restitutions. Ce processus de restitution doit être 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 doit être documentée. À défaut, si ces trois critères ne peuvent être réunis, une étude des risques de ré-identification devra être menée et documentée."*	Les seules productions d'indicateur prévues au sein de l'outil pour le moment sont les graphes d'inclusion et des indicateurs généraux proposés par ce type d'outil de façon native. Ces graphes ne prennent pas en compte des données idenifiante. On pourra documenter ce type de graphe une fois l'outil choisi.
ER-35	Exigence de sécurité SEC-EXP-5	**Hors scope**	**Exportation de données**	Référentiel des EDS de la CNIL	*"Les restitutions mentionnées à l'exigence SEC-EXP-4 doivent être exportées conformément aux exigences SEC-EXP-2 et SEC-EXP-3"*	N/A (les graphes sont intégrés à l'outil et dépendent du droit de visualisation du profil)
ER-36	Exigence de sécurité SEC-SEN-1	**Hors scope**	**Utilisateurs et sécurité**	Référentiel des EDS de la CNIL	*"Chaque personne habilitée à accéder à l'entrepôt doit être formée au respect du secret médical et sensibilisée régulièrement aux risques et obligations inhérents au traitement de données de santé."*	Pas d'impact pour l'outil
ER-37	Exigence de sécurité SEC-SEN-2	**Hors scope**	**Utilisateurs et sécurité**	Référentiel des EDS de la CNIL	*"Chaque personne habilitée à accéder à l'entrepôt doit signer une charte de confidentialité précisant notamment ses obligations au regard de la protection des données à caractère personnel 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"*	Pas d'impact pour l'outil
ER-38	Exigence de sécurité SEC-SEN-3	**Hors scope**	**Utilisateurs et sécurité**	Référentiel des EDS de la CNIL	*"Les postes de travail des personnes habilitées à accéder à l'entrepôt y compris les utilisateurs externes accédant uniquement aux espaces de travail, doivent faire 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. 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 doivent être encadrées au moyen d'une convention entre les parties concernées"*	Pas d'impact pour l'outil
ER-39	Exigence de sécurité SEC-JOU-1	**Faible**	**Journalisation**	Référentiel des EDS de la CNIL	*"Les actions des utilisateurs des espaces de travail de l'entrepôt doivent faire l'objet de mesures de journalisation. En particulier, les connexions à l'entrepôt (identifiants, date et heure), les requêtes et opérations réalisées doivent être tracées."*	Les eCRF ont l'obligation d'avoir un audit trail qui garde trace de toutes les opérations faites sur l'outil. Cette obligation provient du paragraphe 4.9.3/5.5.3des BPC (Bonnes pratiques cliniques *https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000819256*)
ER-40	Exigence de sécurité SEC-JOU-2	**Hors scope**	**Journalisation**	Référentiel des EDS de la CNIL	*"Les accès des ingénieurs et administrateurs système et réseau doivent être 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."*	Les connexions aux machines hébergeant l'outil doivent se faire via une double authentification (éventuellement un bastion d'administration). Ces accès doivent être tracés.
ER-41	Exigence de sécurité SEC-JOU-3	**Faible**	**Journalisation**	Référentiel des EDS de la CNIL	*"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. Ce contrôle doit être réalisé par :* *- une solution réalisant une surveillance automatique avec une remontée d'alertes traitées manuellement par un opérateur habilité ;* *- 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."*	Il semble difficile de mettre en place ce système alors que l'outil gèrera déjà les accès par profils (si cette fonctionnalité fonctionne, une personne ne peut pas accéder à des données qu'il n'est pas censé voir). Un système de type IDS pourrait être envisageable
ER-42	Exigence de sécurité SEC-JOU-4	**Faible**	**Journalisation**	Référentiel des EDS de la CNIL	*"Les traces de journalisation définies aux exigences SEC-JOU-1 et SEC-JOU-2 doivent être conservées pendant une durée de comprise entre 6 mois et un an."*	Les audit trails gardent les traces pour une durée illimitée dans ce type de solution

ER-43	Exigence de sécurité SEC-REI-1	**Faible**	**Ré-identification**	Référentiel des EDS de la CNIL	*"Le responsable de traitement met 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. 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)."*	A voir où les tables de correspondance seront stockées. On devra pouvoir permettre l'exercice des droits des personnes (suppression ou extraction pour transmission)
ER-44	Exigence de sécurité SEC-REI-2	**Hors scope**	**Ré-identification**	Référentiel des EDS de la CNIL	*"Le cas échéant, et en cas de nécessité dûment justifiée et documentée, le responsable de traitement met en place une procédure opérationnelle sécurisée afin de recontacter des patients pour leur proposer de participer à des recherches. 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."*	Pas d'impact pour l'outil
ER-45	Exigence de sécurité SEC-REI-3	**Hors scope**	**Ré-identification**	Référentiel des EDS de la CNIL	*"Le cas échéant, le responsable de traitement met en place une procédure opérationnelle sécurisée afin de ré-identifier des patients en cas d'urgence médicale. 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."*	La procédure dépendra du lieu de stockage des tables de correspondance.
ER-46	Exigence de sécurité SEC-REI-4	**Hors scope**	**Ré-identification**	Référentiel des EDS de la CNIL	*"Les habilitations et accès relatifs aux procédures de ré-identification définies aux exigences SEC-EXC-1 à SEC-EXC-3 doivent être réservés à une équipe restreinte et être limités au strict nécessaire. Les membres de cette équipe restreinte doivent être formés spécifiquement à cette procédure."*	Pas d'impact pour l'outil
ER-47	Exigence de sécurité SEC-REI-5	**Hors scope**	**Ré-identification**	Référentiel des EDS de la CNIL	*"Le responsable de traitement met 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."*	Pas d'impact pour l'outil
ER-48	Exigence de sécurité SEC-INC-1	**Majeure**	**Gestion des incidents**	Référentiel des EDS de la CNIL	*"Le responsable de traitement prévoit une procédure de gestion et de traitement des incidents de sécurité et des violations de données à caractère personnel, précisant les rôles et responsabilités et les actions à mener en cas de survenue de tels incidents"*	Voir avec l'éditeur ou la DSI ce qui sera prévu en cas d'incidents de sécurité ou de violation de données
ER-49	Exigence de sécurité SEC-INC-2	**Hors scope**	**Gestion des incidents**	Référentiel des EDS de la CNIL	*"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 à caractère personnel, doit faire l'objet d'une documentation en interne dans un registre des violations."*	Pas d'impact pour l'outil
ER-50	Exigence de sécurité SEC-INC-3	**Hors scope**	**Gestion des incidents**	Référentiel des EDS de la CNIL	*"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 doit être notifiée à la Commission dans les conditions prévues à l'article 33 du RGPD"*	Pas d'impact pour l'outil
ER-51	Exigence de sécurité SEC-INC-4	**Hors scope**	**Gestion des incidents**	Référentiel des EDS de la CNIL	*"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 est tenu de communiquer la violation des données aux personnes concernées dans les meilleurs délais, conformément à l'article 34 du RGPD."*	Pas d'impact pour l'outil

ER-52	Sous-traitance	**Critique**	Hébergement et sous-traitance	Référentiel des EDS de la CNIL	*"Dans le cas où le responsable de traitement a recours aux services d'un sous-traitant pour l'hébergement, le stockage ou la conservation des données de santé, ce sous-traitant doit être un hébergeur de données de santé agréé ou certifié selon les dispositions du CSP."* *"La mise en place et le fonctionnement d'un entrepôt ne peuvent entrainer le transfert de données à caractère personnel, directement ou indirectement identifiantes hors de l'Union européenne ou à destination d'un pays ne disposant pas d'un niveau de protection adéquat"*	Si mode Saas, alors il faut un **hébergeur français certifié HDS.** Exiger la communication par le prestataire de sa politique de sécurité des systèmes d'information et de ses éventuelles certifications. Cf https://www.cnil.fr/sites/cnil/files/2023-04/cnil_guide_securite_des_donnees_personnelles-2023.pdf Prévoir un contrat encadrant la sous-traitance.
ER-53	Identifiant patient	**Critique**	**Données identifiantes**	Méthodologie de référence MR-00X	*"L'identification des personnes se prêtant à des recherches ne peut être réalisée, dans les bases de données comportant des données de santé à caractère personnel constituées pour la réalisation de la recherche, qu'au moyen d'un numéro d'ordre ou d'un code alphanumérique, établi conformément à l'article 2.2.3, et à l'exclusion de toute donnée à caractère personnel directement identifiante."* *"Lorsque le code alphanumérique se compose de lettres correspondant aux nom et prénom des personnes se prêtant à la recherche, il peut correspondre aux deux premières lettres du nom et à la première lettre du prénom. Il est toutefois recommandé de se limiter aux seules initiales, c'est-à-dire à la première lettre du nom et à la première lettre du prénom. Ces initiales peuvent être complétées d'un numéro d'inclusion et/ou d'un numéro de lieu de recherche ;"*	L'outil doit proposer un système d'**identifiant patient conforme aux MR** (sous la forme numéro lieu de recherche - numéro d'inclusion - initiales)
ER-54	Table de correspondance	**Hors scope**	**Données identifiantes**	Méthodologie de référence MR-001 et MR-003	*"Seuls les professionnels et leurs collaborateurs intervenant dans la recherche dans un lieu de recherche peuvent conserver le lien entre l'identité codée des personnes se prêtant à la recherche utilisée pour associer les données de santé à caractère personnel et leurs nom(s) et prénom(s) (table de correspondance conservée de façon sécurisée)."*	Au même titre que l'exigence SEC-REI-3, cela dépendra du lieu de stockage des tables. Il est intéressant de noter qu'elles doivent être conservées dans les centres recruteurs si on veut être conforme à la MR
ER-55	Destinataire des données identifiantes	**Critique**	**Données identifiantes**	Méthodologie de référence MR-00X	*"[,,,]les catégories de personnes décrites ci-après ont accès aux données traitées, dans les limites de leurs habilitations, au regard de leurs fonctions et dans des conditions conformes à la réglementation:* *- le responsable de traitement et les personnes physiques ou morales agissant pour son compte ; [...]"* *"Peuvent être destinataires de données directement identifiantes concernant les personnes participant à la recherche :* *- les professionnels intervenant dans la recherche et les personnels agissant sous leur responsabilité ou leur autorité, **concernant les personnes dont ils assurent la prise en charge dans le cadre de la recherche** ;[...]"*	L'outil doit permettre de limiter la vision des données directement identifiantes **selon le profil de la personne et selon le centre d'appartenance de la personne** (par ex: un TEC du centre n°3 ne verra que les patients du centre n°3)
ER-56	Consentement	**Faible**	**Consentement**	Méthodologie de référence MR-001	*"Le consentement exprès ou écrit, libre et éclairé, doit être donné par la personne concernée et/ou, le cas échéant, par ses représentant légaux ou personne habilitée à autoriser la recherche, pour participer à la recherche [...]"*	Il pourrait être intéressant qu'on puisse r**ecueillir les consentements au sein de l'outil** (afin notamment de faciliter leur vérification) et d'offrir certaines fonctionnalités autour du consentement de manière dématérialisée (signature en ligne, consultation de document liés à la cohorte...)
ER-57	Droits RGPD	**Hors scope**	**Ré-identification**	Méthodologie de référence MR-00X	*"2.5.2. Modalités d'exercice des droits des personnes se prêtant à la recherche* *Le droit d'accès, prévu par l'article 15 du RGPD peut être exercé à tout moment auprès du professionnel intervenant dans la recherche, directement ou par l'intermédiaire d'un professionnel désigné à cet effet par la personne concernée.* *Conformément aux dispositions de l'article 16 du RGPD, la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes et le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. [...]"*	Garantir les droits RGPD Seule exception pour la MR001: droits à l'effacement (*"Sous réserve d'une information préalable appropriée par le responsable de traitement, certaines données préalablement collectées peuvent cependant ne pas être effacées"*)

ER-58	Conservation des données à caractère personnel dans les MR	**Majeure**	**Conservation des données**	Méthodologie de référence MR-001 (durée diffère selon la MR)	*"Les données à caractère personnel relatives aux personnes se prêtant à une recherche, et traitées à cette fin, ne peuvent être conservées dans les systèmes d'information du responsable de traitement, du centre investigateur ou du professionnel intervenant dans la recherche que jusqu'à la mise sur le marché du produit étudié ou jusqu'à deux ans après la dernière publication des résultats de la recherche ou, en cas d'absence de publication, jusqu'à la signature du rapport final de la recherche. Elles font ensuite l'objet d'un archivage sur support papier ou informatique pour une durée conforme à la réglementation en vigueur."*	L'outil doit permettre de supprimer les données d'un projet (ou les données à caractère personnel)
ER-59	Politique de sécurité et confidentialité	Hors scope	Utilisateurs et sécurité	Méthodologie de référence MR-00X	*"Pour ce faire, il définit, met en œuvre et contrôle l'application d'une politique de sécurité et de confidentialité. Celle-ci pourra notamment décrire, pour la partie concernant les mesures techniques et organisationnelles visant à réduire les risques :* *- les mesures de sécurisation physique des matériels et des locaux ainsi que les dispositions prises pour la sauvegarde des fichiers ;* *- les modalités d'accès aux données, en particulier la gestion des habilitations, les mesures d'identification et d'authentification, les procédures ;* *- les mesures de traçabilité des accès aux informations médicales ainsi que l'historique des connexions ;* *- les mesures de sécurité devant être mises en œuvre pour les transmissions de données."*	Pas d'impact pour l'outil. Prévoir une politique de sécurité et confidentialité
ER-60	Sécurité de l'outil de saisie	Critique	Authentification et contrôle d'accès	Méthodologie de référence MR-00X	*"- dans le cas de la saisie directe des données par les professionnels intervenant dans la recherche ou chez un sous-traitant, l'outil de saisie distante doit être sécurisé en particulier par* ***l'authentification des utilisateurs et le chiffrement des flux de données*** *;"*	Satisfait par les autres exigences du référentiel EDS qui vont plus loin que cette obligation en termes de sécurité
ER-61	Sécurité de l'outil de saisie	Hors scope	Authentification et contrôle d'accès	Méthodologie de référence MR-00X	*"- dans le cas de cahiers d'observation numériques installés sur des dispositifs nomades (tablettes, etc.), les données du traitement doivent être chiffrées dans l'appareil et être protégées par une authentification spécifique de l'utilisateur. Elles doivent pouvoir être transférées uniquement vers le traitement, à travers une liaison sécurisée par authentification et chiffrement des flux ;"*	Pas de saisie prévue par un dispositif nomade.
ER-62	Contrat de sous traitance	Majeure	Hébergement et sous-traitance	Méthodologie de référence MR-00X	*"Lorsque le responsable de traitement fait appel à un ou des sous-traitants, il s'assure que celui-ci présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD, de la loi « Informatique et Libertés » et garantisse la protection des droits de la personne concernée. Le responsable de traitement établit avec le sous-traitant un contrat ou un autre acte juridique précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du règlement général sur la protection des données. En particulier, le contrat doit prévoir que le sous-traitant :[...]"*	Prévoir dans le cadre de la contractualisation les obligation du sous traitant
ER-63	Audit du sous traitant	Faible	Hébergement et sous-traitance	Méthodologie de référence MR-00X	*"Pour tout projet commencé avec un nouveau sous-traitant (n'ayant pas la qualité de lieu de recherche), un audit est effectué. Il couvre notamment la vérification des plans qualité et sécurité de l'entreprise, la validation des systèmes informatiques avec l'existence d'un système de sauvegarde et de récupération des données, et de mesures destinées à garantir leur confidentialité et leur intégrité."*	Voir si l'éditeur a valeur de sous traitant et doit être audité
ER-64	Utilisation de CSP	Majeure	Réseau	Guide ANSSI Sécurisation site web	*"L'ANSSI a publié sur son site des recommandations spécifiques pour mettre en œuvre TLS ou pour sécuriser un site web."*	- Utilisation du mécanisme de sécurité standardisé CSP ("Content Security Policy") dans l'application web - Utiliser le mécanisme de sécurité HSTS ("HTTP Strict Transport Security")
ER-65	Utilisation d'IDS	Majeure	Réseau	Guide CNIL sécurité des données personnelles	*"Des systèmes de détection d'intrusion (IDS) peuvent analyser le trafic réseau pour détecter des* *attaques. Les utilisateurs doivent être avertis lorsque leurs contenus sont analysés."*	Utiliser un système de détection d'intrusion serait un plus pour repérer les activités suspectes ou inhabituelles sur l'outil

ER-66	Mise à jour des systèmes	Majeure	Hébergement et sous-traitance	Guide CNIL sécurité des données personnelles	"Installer les mises à jour critiques sans délai que ce soit pour les systèmes d'exploitation ou pour les applications, en programmant une vérification automatique hebdomadaire"	Prévoir plan de maintenance et application des mises à jour critique de manière régulière
ER-67	Sauvegardes	Majeure	Hébergement et sous-traitance	Guide CNIL sécurité des données personnelles	"S'agissant de la sauvegarde des données - Effectuer des sauvegardes fréquentes des données - Stocker les sauvegardes sur un site extérieur, si possible dans des coffres ignifugés et étanches. - Protéger les données sauvegardées au même niveau de sécurité que celles stockées sur les serveurs d'exploitation - Lorsque les sauvegardes sont transmises par le réseau, il convient de chiffrer le canal de transmission si celui-ci n'est pas interne à l'organisme." "S'agissant de la reprise et de la continuité d'activité: - Rédiger un plan de reprise et de continuité d'activité informatique même sommaire, incluant la liste des intervenants. - S'assurer que les utilisateurs, prestataires et sous-traitants savent qui alerter en cas d'incident. - Tester régulièrement la restauration des sauvegardes et l'application du plan de continuité ou de reprise de l'activité. À propos des matériels : - utiliser un onduleur pour protéger le matériel servant aux traitements essentiels ; - prévoir une redondance matérielle des matériels de stockage, par exemple au moyen d'une technologie RAID"	Prévoir les paramètres de sauvegarde ou vérifier leur existence (sauvegarde régulière (journalière), stockage sur site extérieur, chiffrement des données, test régulier) Prévoir ou vérifier l'existence d'un PRA
ER-68	BPC 5.5	Critique	Gestion des incidents	Bonnes pratiques cliniques	*5.5.3. Si les données de la recherche biomédicale font l'objet d'un traitement ou sont gérées par des systèmes informatisés, le promoteur :* *a) S'assure et documente le fait que les systèmes informatisés utilisés dans la recherche sont conformes aux exigences qu'il a établies en matière d'intégrité, d'exactitude, de fiabilité des données et de respect des performances attendues (c'est-à-dire la validation) ;* *b) Met en place et assure le suivi des procédures opératoires standardisées relatives à l'utilisation de ces systèmes ;* *c) S'assure que la conception de ces systèmes permet la modification de données de telle sorte que les modifications soient documentées et qu'aucune donnée saisie ne soit supprimée (c'est-à-dire conserve un tracé d'audit des données et des modifications) ;* *d) Met en place et assure le suivi d'un système de sécurité qui empêche tout accès non autorisé aux données ;* *e) Tient à jour la liste des personnes autorisées à modifier les données (voir 4.1.5 et 4.9.3) ;* *f) Effectue des copies de sauvegarde appropriées des données ;* *g) Préserve l'insu, s'il y a lieu (par exemple lors de la saisie et du traitement des données) ;* *h) S'assure que les traitements de données à caractère personnel mis en oeuvre dans le cadre de la recherche sont réalisés dans les conditions définies par la loi n° 78-17 du 6 janvier 1978 susvisée et des textes réglementaires pris pour son application et, le cas échéant, la décision de la Commission nationale de l'informatique et des libertés du 5 janvier 2006 portant homologation d'une méthodologie de référence pour les traitements de données personnelles opérées dans le cadre des recherches biomédicales.*	Hormis l'obligation de VSI, les différentes obligations des BPC (audit trail, sécurité, revue d'habilitation, sauvegarde, insu) sont assurées par les textes vus précedemment.

ER-69	BPC 4.9.3 et 4.14.1	Critique	Conservation des données	Bonnes pratiques cliniques	*4.9.3 Toute modification ou correction apportée à un cahier d'observation est datée et paraphée par l'investigateur ou une personne désignée par lui, et ne doit pas masquer l'inscription originale (c'est-à-dire qu'un tracé d'audit doit être conservé) ; les raisons des modifications sont indiquées si nécessaire. Cela s'applique aux modifications et corrections effectuées quel que soit le support (voir 5.18.4 [n]). Le promoteur fournit des consignes aux investigateurs ou aux personnes que ces derniers auront désignées pour faire ces corrections. Le promoteur dispose de procédures écrites afin de garantir que les modifications ou corrections apportées aux cahiers d'observation par des représentants qu'il a désignés ont été documentées, qu'elles sont nécessaires et ont l'approbation de l'investigateur. L'investigateur conserve une trace écrite des modifications ou corrections effectuées.* *4.14.1. Les investigateurs et toutes personnes appelées à collaborer aux essais sont tenus au secret professionnel conformément aux dispositions législatives et réglementaires en vigueur, notamment l'article R. 5121-13 du code de la santé publique.* *Pendant la recherche biomédicale et à son issue, les données recueillies sur les personnes qui s'y prêtent et transmises au promoteur par les investigateurs (ou tous autres intervenants spécialisés) ne doivent en aucun cas faire apparaître en clair les noms des personnes concernées, ni leur adresse, ni d'autre information permettant une identification directe.*	Couvert par les exigences sur l'audit trail, et l'accès aux données identifiantes en fonction du centre d'appartenance de la personne