Analyse d'impact relative à la protection des données personnelles SOG HEALTH réutilisées dans le cadre du projet sur le recours en vie réelle à la vaccination contre le Chikungunya en France hexagonale – Valneva France SAS

Table des matières

Chapitre I. INTRODUCTION

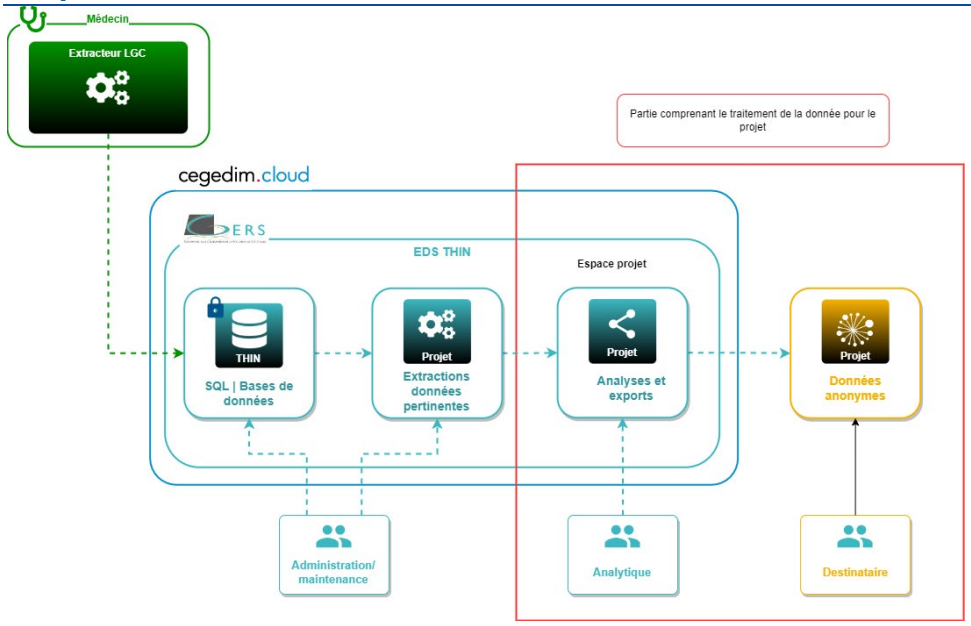
Cette analyse d'impact relative à la protection des données est menée dans le cadre du projet sur le recours en vie réelle à la vaccination contre le Chikungunya en France hexagonale réalisé sur les données de l'EDS SOG HEALTH, qui contient des données de délivrances et de ventes en vie réelle en provenance des logiciels de gestion d'officine de pharmacie.

L'ensemble des traitements concernant l'EDS SOG HEALTH a été présenté et validé par la CNIL au moment de la décision DT-2025-014 autorisant la mise en place de l'entrepôt.

Les responsabilités suivantes ont été établies dans le cadre de la réalisation du projet sur le le recours en vie réelle à la vaccination contre le Chikungunya en France hexagonale :

Co-Responsable du traitement 1	**VALNEVA France SAS,** qui détermine les finalités de l'étude Nom de la personne en charge : Nicolas Arvis – VP general Manager France-benelux-Iberia DPO : Nicole Urban-Krenn
Co-responsable du traitement 2	**Clinityx by GERS data** Nom de la personne en charge : Nicolas Glatt - Directeur Général DPO : Laurène Gantzer
Responsable de mise en œuvre du traitement	**Clinityx by GERS data** Nom de la personne en charge : Nicolas Glatt - Directeur Général DPO : Laurène Gantzer
Sous-traitant Clinityx by GERS data	**Cegedim.cloud**, en charge de l'hébergement et de l'infogérance du système d'information de Clinityx by GERS data Infogéreur certifié HDS (hébergeur de données de santé) 1.1, SecNumCloud, ISO 27001, ISO 27018, ISAE 3402 type II, soit le plus haut niveau de certification en vigueur.

Cette analyse d'impact porte sur les traitements mis en œuvre dans le cadre du projet le recours en vie réelle à la vaccination contre le Chikungunya en France hexagonale, à savoir la partie encadrée rouge du schéma ci-dessous :



Chapitre II. PROPORTIONNALITE ET NECESSITE DU TRAITEMENT

Finalités : déterminées, explicites et légitimes	
Suivre l'usage en vie réelle des vaccins dans la prévention de l'infection par le CHIKV en France hexagonale à partir d'indicateur concernant les données générales (patients & prescripteurs). Ces données permettront de mieux définir les populations déjà vaccinées et ainsi préciser le profil de sécurité en vie réelle du vaccin dans les diverses populations vaccinées	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Fondement : licéité du traitement, interdiction du détournement de finalité	
Les projets CLINITYX BY GERS DATA sont soumis au comité scientifique qui évalue le caractère éthique et légitime de chacun. Le fondement du traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement (article 6.1 du RGPD). Les responsables de traitement (RT) se sont engagés contractuellement à la garantie de non-poursuite des finalités interdites.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Minimisation des données : adéquates, pertinentes et limitées	
Seules les données pertinentes dans le cadre du projet sont mises à disposition des personnes CLINITYX BY GERS DATA habilitées à travailler sur le projet. Les critères d'inclusion sont décrits dans la fiche projet jointe.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Qualité des données : exactes et tenues à jour	

Chapitre III. MESURES PROTECTRICES DES DROITS DES PERSONNES CONCERNEES

Un contrôle qualité est assuré à l'intégration des données dans l'EDS. Il consiste à vérifier le format et l'existence des codes produits, codes actes, etc., ainsi que les quantités pour éliminer d'éventuelles valeurs aberrantes. Un procédé de quality assessment est également effectué sur la base de données et tourne mensuellement. Il porte sur des indicateurs de contrôle spécifiques, comme les volumes des factures au mois le mois et au total, la distribution de ces indicateurs par pharmacie, les volumes de produits par classe thérapeutique... Par ailleurs, à la mise à disposition des données dans l'espace projet, les data analystes CLINITYX BY GERS DATA habilitées à travailler sur le projet vérifient la cohérence des données et réappliquent des nettoyages nécessaires si besoin.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Durées de conservation : limitées
La durée de conservation établie dans le cadre du projet sur le recours en vie réelle à la vaccination contre le Chikungunya en France hexagonale de Valneva France SAS est de 24 mois. A l'issue de cette durée, les données seront supprimées.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Chapitre III. MESURES PROTECTRICES DES DROITS DES PERSONNES CONCERNEES

Information des personnes (traitement loyal et transparent)
Les personnes ont été informées conformément aux mentions prévues par dans les articles 12 à 14 du RGPD. Dans le cadre de la réutilisation des données d'un entrepôt d'un EDS, le mécanisme d'information dynamique s'opère : le patient est initialement informé individuellement de la collecte de ses données dans le cadre de l'EDS. Il peut ensuite consulter l'ensemble des projets dans lesquels ses données ont pu être réutilisées via le portail de transparence de Clinityx by GERS DATA https://www.gers-sas-transparence.com/Pages/home.aspx.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Recueil du consentement
La licéité du présent traitement ne repose pas sur le consentement mais sur l'information préalable des personnes conformément aux dispositions du RGPD (voir *supra*), et dans le cadre d'un entrepôt de données de santé autorisé par la CNIL.

Evaluation de la mesure	**Non applicable**
Mesure corrective	NA

Exercice des droits d'accès et à la portabilité
Pas au niveau de l'espace projets*

Evaluation de la mesure	**Non applicable**

Chapitre IV. MESURES DE SECURITE AUTOUR DU TRAITEMENT

Mesure corrective	NA
Exercice des droits de rectification et d'effacement	
Pas au niveau de l'espace projets*	
Evaluation de la mesure	**Non applicable**
Mesure corrective	NA
Exercice des droits de limitation du traitement et d'opposition	
Pas au niveau de l'espace projets*	
Evaluation de la mesure	**Non applicable**
Mesure corrective	NA
Sous-traitance : identifiée et contractualisée	
La relation entre CLINITYX BY GERS DATA et Valneva France SAS agissant en qualité de RT a été identifiée et contractualisée.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	
Aucun transfert de données hors de l'Union européenne dans le cadre du projet.	
Evaluation de la mesure	**Non applicable**
Mesure corrective	NA

**L'exercice des droits des personnes s'exerce au niveau de l'EDS SOG HEALTH selon les modalités validées avec la CNIL dans le cadre de l'autorisation EDS SOG HEALTH et non de la partie projets. Les personnes concernées n'exercent en effet pas leur droit au niveau de la partie projets, mais de l'ensemble des données SOG HEALTH.*

Chapitre IV. MESURES DE SECURITE AUTOUR DU TRAITEMENT

CLINITYX BY GERS DATA, en tant que responsable de mise en œuvre du traitement, s'engage à ce que la description de l'ensemble des traitements de ce chapitre soit exacte et tenue à jour.

IV.1. Evaluation des mesures contribuant à traiter des risques liés à la sécurité des données

Cloisonnement	
Pour toute l'infrastructure gérée par le sous-traitant cegedim.cloud, les traitements sont dans des VLANs dédiés sur des serveurs dédiés aux traitements. L'accès à tous les serveurs se fait par le biais du bastion Wallix.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Chiffrement	
• Au niveau du transport : protocole RSA-2048 bits et TLS 1.2/1.3 • Au niveau du stockage : AES-256 at rest • Au niveau des données : chiffrement AES-256	

Chapitre IV. MESURES DE SECURITE AUTOUR DU TRAITEMENT

• Hachage des ID patients et médecins : SHA-256	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Filtrage	
- Flux à l'intérieur des VLANs : chiffrés au niveau du transport par un protocole RSA-2048 bits et TLS 1.2/1.3. - Flux entre processus dans les VLANS et à l'extérieur : protégés par firewall.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Archivage/ durées de conservation des données à chaque étape du traitement	
L'effacement dans l'environnement cegedim.cloud correspond au standard NIST 800-88. Les fichiers de données spécifiques à un projet sont conservés dans le bucket dédié au projet pendant 24 mois après finalisation de l'étude, en cas de besoin de vérification ou d'analyses complémentaires. A l'issue des 24 mois, ils sont supprimés de l'espace projet. A chaque réunion du comité de pilotage de l'EDS, les espaces de stockage projet sont passés en revue pour s'assurer que la règle de conservation des données d'études est bien respectée.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Traçabilité – Journalisation	
Tous les environnements cegedim.cloud sont protégés derrière un bastion Wallix. La traçabilité des actions est assurée dans les conditions prévues par cegedim.cloud via le bastion Wallix. Notamment, des traces fonctionnelles sont mises en place sur le bastion afin de suivre les activités des utilisateurs au travers d'enregistrements des sessions, qui sont conservés 30 jours dans les systèmes. Sur chaque équipement d'infra, des traces techniques sont gérées par cegedim.cloud. Elles sont conservées 60 jours dans les systèmes. Les traces fonctionnelles et techniques sont conservées 1 an en archive. Par ailleurs, une surveillance automatique des logs est effectuée via OpenSearch, avec relecture manuelle par un administrateur.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Contrôle d'intégrité	
Sur toutes les étapes d'échange des fichiers, un contrôle d'intégrité est opéré par la fonctionnalité native de dépôt et retrait des données de l'espace de stockage objet sécurisé.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Contrôle des accès logiques	
Tous les environnements de l'EDS sont derrière un bastion Wallix. Il y a un bastion distinct pour CLINITYX BY GERS DATA (administration de l'EDS) et pour la partie projets de CLINITYX BY GERS DATA. Chaque personne doit non seulement avoir des identifiants de l'Active Directory de CLINITYX BY GERS DATA mais également des identifiants spécifiques pour accéder au bastion.	

Chapitre IV. MESURES DE SECURITE AUTOUR DU TRAITEMENT

Les mots de passe doivent comporter 12 caractères minimum, être alphanumériques (et sensibles à la casse) avec obligation de contenir des caractères spéciaux. La durée de validité maximum est de 42 jours. Les comptes se bloquent après 5 tentatives.
Les autorisations d'accès s'inscrivent dans le cadre d'un processus d'autorisation formalisé impliquant RH, RSSI et Direction métier. Les accès sont distribués après engagement formel de l'utilisateur à respecter les règles de sécurité, notamment celles relatives à la protection des moyens d'accès. La distribution de droit d'accès est effectuée uniquement sur demande motivée d'une personne disposant des habilitations nécessaires. La demande est tracée.
En cas de départ d'un collaborateur ou de changement de mission ou de retrait d'habilitation, les droits d'accès sont immédiatement retirés. Le sas d'administration au bastion se compose de quatre composants principaux :

- Le bastion d'administration (proxy RDP/SSH, traçabilité des sessions) ;
- Le service d'authentification forte (MFA – Multi Factors Authentication) ;
- L'annuaire des comptes d'administration ;
- Les serveurs de rebond, sur lesquels sont installés les outils d'administration. L'accès aux serveurs de rebond est automatique une fois connecté au bastion.

Des profils utilisateurs différents sont définis en fonction des rôles (administrateurs / data engineer / data analystes) donnant des droits d'accès différents aux données à chaque étape du traitement.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Anonymisation

Aucune donnée brute ne sort de l'EDS ou n'est transmise à des tiers en dehors de l'équipe de data analystes de CLINITYX BY GERS DATA en charge des projets.
L'anonymat des résultats fournis sous forme de tableaux ou graphiques de données agrégées est vérifié au préalable au regard des critères recommandés par le Comité européen de la protection des données dans le document Opinion 05/2014 on Anonymisation Techniques du 10 avril 2014.
Le responsable du service études de CLINITYX BY GERS DATA est en charge de la vérification du caractère anonyme des données pour chaque étude produite avant diffusion aux destinataires.
Par ailleurs, avant chaque sortie de données de l'EDS, le responsable d'étude CLINITYX BY GERS DATA en charge du projet doit valider la grille suivante :

Chapitre IV. MESURES DE SECURITE AUTOUR DU TRAITEMENT

Condition	Validation
Aucun agrégat contenant moins de 30 clients (résultat extrapolé) n'est restitué	☐ Vrai ☐ Faux
Le risque d'inférence a été considéré par le responsable de projets comme étant nul	☐ Vrai ☐ Faux
Aucun agrégat au niveau d'une zone géographique contient moins de 5 établissements n'est restitué	☐ Vrai ☐ Faux
Validation de la grille *(oui ou vrai à tous les éléments)*	OUI NON *Note : si **Non**, le projet est **invalidé***

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Sécurité des documents papiers	
Le traitement des données SOG HEALTH ne contient pas de document papier	
Evaluation de la mesure	**Non applicable**
Mesure corrective	NA

IV.2. Evaluation des mesures générales de sécurité

Sécurité de l'exploitation	
La couche infra OS est gérée par cegedim.cloud – pour les processus de gestion des changements et des vulnérabilités. Ces processus sont certifiés ISO 27001 (système de management de la sécurité de l'information), ISO 27017 (système de management de la sécurité des services cloud), ISO 27018 (protection des données à caractère personnel dans les services cloud) et HDS v1.1 (hébergement des données de santé) : activités 1 à 6 incluses.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Lutte contre les logiciels malveillants	
Les serveurs et postes de travail sont munis d'une protection permanente et à jour contre les virus et les logiciels malveillants. Les postes de travail des collaborateurs ainsi que l'ensemble des serveurs Windows et Linux sont équipés d'une solution antivirale de nouvelle génération, SentinelOne, intégrant un EDR ("Endpoint Detection and Response") ainsi que d'une solution d'analyse comportementale (UEBA). Les évènements générés par ces solutions sont surveillés en 24/7 par le SOC de Cegedim.cloud. La solution antivirale n'est pas basée sur des signatures mais sur des moteurs d'analyse comportementale couplés à de l'intelligence artificielle. La solution EDR assure une traçabilité complète des évènements du système (fichiers, connexion réseau, exécution de processus., etc.). L'antivirus vérifie la réputation et le comportement des fichiers via des	

Chapitre IV. MESURES DE SECURITE AUTOUR DU TRAITEMENT

algorithmes locaux et l'interrogation de la console antivirus en temps réel si le poste ou le serveur dispose d'une connectivité avec celle-ci. L'antivirus contrôle les fichiers créés, modifiés, exécutés. Il contrôle également les pièces jointes et les médias amovibles dès leur connexion.La messagerie fait l'objet de contrôles antivirus et anti-spam.Les passerelles d'accès Internet (proxy) font l'objet de contrôles antivirus. La solution Forcepoint Firewall complète le dispositif anti-intrusion sur les postes et serveurs de l'infrastructure.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Gestion des postes de travail	
Les postes de travail sont masterisés par cegedim.cloud : tous les postes sont chiffrés avec antivirus, pare-feu, désactivation de l'autorun des ports USB et surveillance des applications installées. Le stockage des postes de travail est chiffré. Aucune donnée critique est stockée sur le poste de travail.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Sécurité des sites web	
Il n'y a pas de site web dans le cadre du traitement.	
Evaluation de la mesure	NA
Mesure corrective	NA
Maintenance	
Les équipements data centers et postes de travail sont gérés par cegedim.cloud (cf. partie « Sécurité de l'exploitation » plus haut dans le tableau). Les interventions de maintenance sont enregistrées sur une main courante. Toutes les interventions de maintenance des matériels réalisées par un sous-traitant se font en présence d'une personne de cegedim.cloud. Les matériels ne sortent pas du data center pour réparation. Ils sont réparés sur place. En cas de sortie des supports de stockage pour destruction, recyclage ou don, les supports sont reconditionnés et contrôlés pour s'assurer qu'aucune donnée n'est encore présente dessus. Ces opérations font l'objet d'un Request For Change validé en Comité d'Approbation des Changements.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Sauvegardes	
Cegedim.cloud met en œuvre un processus de sauvegarde de telle sorte que : • Les sauvegardes quotidiennes sont systématiquement testées lors de la sauvegarde afin de vérifier leur fiabilité, • Le bon dimensionnement des dispositifs de sauvegarde est vérifié régulièrement par les administrateurs, • Un test de restauration des sauvegardes sur une machine de test peut être effectué à la demande des directions métiers,	

Chapitre IV. MESURES DE SECURITE AUTOUR DU TRAITEMENT

- Les matériels et médias de sauvegarde font l'objet de mesures de protection physique et logique, les médias étant stockés dans des locaux sécurisés éloignés des locaux où sont installés les serveurs.

Les supports de stockage sont par ailleurs chiffrés avec AES 256. Le type de support est SAN.
Les machines virtuelles font l'objet d'une sauvegarde quotidienne. Les sauvegardes de ces machines ont une durée de rétention de 28 jours.
Les bases de données font l'objet d'une sauvegarde quotidienne. Les sauvegardes de ces bases ont une durée de rétention de 15 jours.
Il existe une réplication en temps réel sur le site miroir.
Le logiciel Rubrik permet de faire la sauvegarde et la partie réplication.
La bonne réalisation des sauvegardes et de la réplication sur site miroir est monitorée par la solution Centréon.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Sécurité des canaux informatiques (réseaux)

Les principes généraux de sécurité réseau appliqués sont les suivants :

- Tout flux passant d'un réseau à un autre, passe à minima par un firewall ;
- Principe de "Refus par défaut" : tout flux qui n'est pas spécifiquement autorisé est interdit ;
- Les firewalls sont protégés physiquement ;
- Les firewalls sont un élément de la stratégie globale de défense en profondeur ;
- Les firewalls ne doivent pas être inutilement complexes. La simplicité d'un système facilite sa gestion et son audit ;
- Les firewalls sont l'implémentation technique de la politique de sécurité réseau de Cegedim.cloud

L'ensemble des principes de sécurité sont détaillés dans la politique de sécurité réseau de cegedim.cloud.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Surveillance

La surveillance s'effectue via les équipements de filtrage des flux (firewall, proxys), et au travers d'une analyse via les sondes IDS/IPS.
Le contrôle des configurations matérielles est assuré par le processus gestion des configurations et l'outil IT Care.
La gestion des configurations logicielle sur les postes de travail s'effectue via Workspace One.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Contrôle d'accès physiques

Trois types de zones sont définis pour les accès physiques :

- Public : accueil, voie publique, etc.

- Privé : les bureaux – accès par badge individuel
- Sensible : les data centers et les salles techniques – accès par badge individuel avec biométrie. Les zones sensibles sont en outre sous vidéo surveillance

Des dispositifs de détection et de réponse aux intrusions sont en place quelle que soit la zone. Des rondes sont effectuées par du personnel de surveillance, ainsi que par un centre de surveillance des alertes avec une astreinte 24h/24 et 7j/7.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Sécurité des matériels

L'ensemble des actifs manipulés au sein du groupe Cegedim, qu'il s'agisse des actifs internes Cegedim ou des actifs des clients, le sont en accord avec leur niveau de sensibilité. L'utilisation correcte des actifs est encadrée par un corpus documentaire (PSSI, Charte SSI, guide sécurité, etc.) et via les moyens techniques et organisationnels adaptés au niveau de sensibilité de l'actif considéré. Les utilisateurs du système d'information du groupe Cegedim sont sensibilisés aux pratiques applicables en termes d'utilisation correcte des actifs.
Les postes portables sont sécurisés via câble antivol.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Eloignement des sources de risque

Actuellement, les locaux du data center sont en zone d'inondation à cause de la nappe phréatique au niveau du data center mais cegedim.cloud a mis en œuvre des moyens de sécurisation de l'emplacement contre ce type de sinistres.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Protection contre les sources de risque non humaines

Les moyens mis en œuvre sont les suivants :

- Lutte contre le feu :
  - Prévention : pas de stockages de matières inflammables à proximité des zones de chaleurs et zones sensibles
  - Détection : sondes et des détecteurs reliés à la console centralisée et remontent des alertes. La console est monitorée en 24/7
  - Réaction : Systèmes automatisés d'extinction au gaz dans les data centers
- Risques électriques :
  - Prévention : mise en place de deux boucles d'alimentation électrique dans les data centers, distinction entre les courants forts et les courants faibles ainsi qu'équipements critiques sous des onduleurs
  - Détection : contrôle des tensions. Les équipements permettent de mesurer et de répondre aux problèmes de sous tension et sur tension
  - Réaction : les onduleurs prennent le relai – en cas de coupures, les groupes électrogènes démarrent
- Gestion de la température et de l'hygrométrie :

○ Prévention : assurée par un monitoring de la température et de l'humidité sur une console centralisée reliée aux équipements de chauffage et de climatisation ○ Détection : sondes de fuite d'eau dans les salles techniques et data centers également rattachés aux consoles de monitoring ○ Réactions : si dépassement des seuils, la climatisation, les pompes et les déshumidificateurs se mettent en marche.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Chapitre V. MESURES ORGANISATIONNELLES ET GOUVERNANCE DE LA DONNEE

Organisation	
Un DPO est nommé sur le périmètre et dispose des moyens nécessaires pour assurer sa mission. Des réunions relais DPO sont réalisées entre les DPOs des responsables de traitement et de ses sous-traitants ainsi qu'avec les directions juridiques de chacun pour évaluer la situation et les évolutions souhaitées, acter des décisions et suivre l'avancement de leur exécution. Au niveau de la sécurité, des référents sécurité sont nommés avec un back-up. Un point de suivi mensuel est organisé entre les DPO.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Politique (gestion des règles)	
La politique de gestion des règles est traduite dans les documents suivants : • Charte de sécurité des SI signée par tous les utilisateurs (collaborateurs internes et prestataires) ; • Charte de confidentialité signée par tous les utilisateurs (collaborateurs internes et prestataires) ; • Politique de sécurité des SI groupe (applicable à l'ensemble des entités et des personnels) ; • Politique de protection des données personnelles groupes (applicable à toutes les entités et leurs personnels). CLINITYX BY GERS DATA, Cegedim Santé et cegedim.cloud en tant que filiales du Groupe Cegedim sont soumises à cette politique.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Gestion des risques	
Une politique de gestion des risques est menée au sein du groupe Cegedim et s'applique à toutes les filiales avec un processus d'évaluation du risque :	

Chapitre V. MESURES ORGANISATIONNELLES ET GOUVERNANCE DE LA DONNEE

- Validation par RSSI Adjoint, Directeur juridique et Direction Générale du groupe ;
- Applicable à l'ensemble des entités du groupe ;
- Gérés en accord avec les standards internationaux, conformément aux contraintes contractuelles, normatives, légales et réglementaires applicables.

La documentation suivante est tenue à jour :

- Tenue d'un registre des traitements par les responsables de traitement ;
- Tenue d'un registre des traitements chez les sous-traitants.

Tous les risques sécurité sont également réévalués tous les ans (Ebios RM).

De même, l'AIPD concernant l'EDS est revue à minima tous les ans.

La gestion d'un plan d'actions sécurité est également en place.

CLINITYX BY GERS DATA et cegedim.cloud en tant que filiales du Groupe Cegedim sont soumises à cette politique.

Par ailleurs, une AIPD complétée par une analyse de risque est réalisée pour chaque projet.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Gestion des projets

Tout projet d'études à partir des données de la base SOG HEALTH fait l'objet d'une soumission par formulaire en suivant un protocole spécifique et adressé au Comité Scientifique pour l'évaluation et la faisabilité du projet.

- La demande comporte une description de son organisme et de ses activités, une déclaration de liens et intérêts du porteur de projet, et un résumé du projet comportant les objectifs du projet, la méthode proposée, une description des données nécessaires, le cadre réglementaire du projet, les modalités et un calendrier de réalisation.
- Le comité scientifique justifie et documente chacun des points suivants avant validation d'un projet :
  - La faisabilité du projet ;
  - La pertinence scientifique et stratégique ;
  - La validité de la méthodologie au regard des objectifs ;
  - Le caractère éthique ;
  - Le bénéfice attendu pour les patients concernés ;
  - Le caractère d'intérêt légitime ou public ;
  - Dans le cas où le porteur de projet est un industriel de santé ou un assureur de santé, l'absence de poursuite de finalités interdites mentionnées à l'article L.1461-3 du Code de la santé.
- Le Comité rend son avis par écrit au porteur de projet dans un délai de 4 semaines. En cas d'avis défavorable, celui-ci est justifié au Porteur de projet. Seuls les projets ayant reçu un avis favorable peuvent être menés.

Chapitre V. MESURES ORGANISATIONNELLES ET GOUVERNANCE DE LA DONNEE

Evaluation de la mesure	NA
Mesure corrective	NA

Gestion des incidents et violations des données

Des procédures existent au sein de la PSSI du Groupe Cegedim. CLINITYX BY GERS DATA, ainsi que cegedim.cloud en tant que filiales sont soumises à ces procédures. Les procédures concernant la violation des données personnelles sont déclinées dans chacune des entités.
La gestion des incident et violation des données contient notamment les mesures suivantes :

- Procédures de prévenance de tout incident de sécurité, en conformité avec l'article 33 du RGPD :
  - Notification du sous-traitant aux responsables de traitement de toute violation des données dans les meilleurs délais après en avoir pris connaissance ;
  - Information des responsables de traitement de cette violation des données à la CNIL au plus tard dans les 72h après en avoir été lui-même informé et description de la nature de la violation, ses conséquences probables et les mesures prises pour y remédier.
- Procédures de prévenance des personnes concernées par la violation des données à caractère personnel, conformément à l'article 34 du RGPD.

Un e-learning est également en place pour sensibiliser les collaborateurs aux violations de données personnes et à la conduite à adopter en cas d'incident.
Des exercices de simulation gestion de crise sont régulièrement réalisés par les RSSI pour s'assurer des acquis des collaborateurs et dans un processus d'amélioration continu.

Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Gestion des personnels

Le groupe Cegedim dispose d'une politique de sensibilisation de l'ensemble des collaborateurs au RGPD. CLINITYX BY GERS DATA et cegedim.cloud en tant que filiales sont soumises à cette politique.

Voici le descriptif de mesures relatives à la gestion des personnels :

- Charte et contrat de travail qui rappellent les obligations de protection de la donnée et de confidentialité de la donnée ;
- Charte de confidentialité signée par les utilisateurs habilités à accéder à l'EDS ;
- Sensibilisation au secret médical ;
- Sensibilisation concernant les données de santé ;
- Des e-learning obligatoires sur les sujets de RGPD et de protection/violation des données ;
- Sécurité : sensibilisation aux bonnes pratiques sur la charte, avec une réévaluation annuelle ;

Chaque e-learning a un quizz obligatoire avec une note minimale à atteindre qui permet de déterminer si l'apprenant a une bonne compréhension du sujet

Chapitre V. MESURES ORGANISATIONNELLES ET GOUVERNANCE DE LA DONNEE

Les sessions de sensibilisation et de e-learning et des évaluations ont lieu tous les ans au dernier trimestre de l'année. Pour tous : les résultats sont suivis mensuellement.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Relation avec les tiers	
La relation avec cegedim.cloud est encadrée contractuellement. La relation entre Valneva France SAS, et CLINITYX BY GERS DATA est encadrée, selon un contrat client type est élaboré avec la direction juridique et revu régulièrement.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA
Supervision	
Une supervision est réalisée via les AIPD et des déclenchements ponctuels d'audits internes.	
Evaluation de la mesure	**Acceptable**
Mesure corrective	NA

Chapitre VI. ETUDE D'IMPACT DES ATTEINTES POTENTIELLES A LA VIE PRIVEE

VI.1. Analyse et estimation des risques

1.1. Accès illégitime à des données

1.1.1. Principales sources de risque

- Cybercriminel (revente de données, chantage à l'exfiltration, usurpation d'identité),
- Concurrence (pré-positionnement stratégique, dénigrement…),
- Activiste idéologique (s'opposer à des projets de recherche, démontrer une faille de sécurité dans la plateforme),
- Puissance étrangère (renseignement),
- Malveillant dans l'entourage (interne, ou client pour faire de la campagne d'influence),
- Erreur de configuration amenant à une exposition publique des données.

1.1.2. Principales menaces

- Interception de flux (un attaquant se place entre les pharmacies et CLINITYX BY GERS DATA ou entre CLINITYX BY GERS DATA et le client),
- Défaut de cloisonnement logique (VLAN non étanche et porosité entre les VLANs),
- Défaut de contrôle d'accès (plus de droits que nécessaires) ou facilitation d'une élévation de privilèges,
- Crédulité des acteurs (manque de sensibilisation, plus susceptible d'être victime d'une attaque en ingénierie sociale).

1.1.3. Principaux impacts potentiels

- Accès illégitime sans ré-identification : anxiété et stress de voir ces données ré-identifiées et l'orientation médicale des personnes dévoilées, notamment si ces informations n'étaient pas connues de l'entourage direct ou indirect de la personne
- Accès illégitime avec ré-identification :
    - Préjudice moral liée à la révélation de l'orientation médicale des patients (stigmatisation personnelle ou professionnelle, préjugés)
    - Discrimination (professionnelle, d'assurances)
    - Conséquences psychologiques dues aux discriminations (stress, anxiété, angoisse)
    - Possibilité d'être cible d'une attaque ciblée (type phishing ou autre)
    - Perte de confiance dans le système de santé – et notamment les fournisseurs de soins de santé (les médecins)

1.1.4. Principales mesures réduisant la gravité et la vraisemblance

La donnée SOG HEALTH est pseudonymisée à plusieurs étapes du traitement, notamment à la source sur les logiciels de gestion d'officine. L'EDS ne contient pas de données directement identifiantes. Des codes aléatoires non signifiants étant générés lors de l'extraction des données au niveau des LGOs, aucune table de correspondance n'existe entre des informations directement identifiantes du patient et les codes aléatoires générés.

De même, les codes prescripteurs sont hachés à la source et re-hachés par la suite, rendant la réversibilité impossible à mettre en place, notamment en complément des autres mesures de sécurité telles que le cryptage et le cloisonnement mises en place autour du traitement de la donnée.

Seule les données pertinentes dans le cadre du projet sont mises à disposition dans l'espace projet. Il s'agit donc d'un sous ensemble de <1% patients, ne comprenant pas l'ensemble des données disponibles dans la base SOG HEALTH. La sélection et l'appauvrissement des données effectuée dans le cadre du projet rendent donc la probabilité de réidentification extrêmement faible.

Tous les flux sont sécurisés, et la donnée est cryptée, rendant illisible le contenu et demandant des efforts disproportionnés à l'attaquant afin de décrypter les données.

Les données sont traitées dans des environnements cloisonnés selon le plus haut niveau de sécurité en vigueur, avec des règles strictes de contrôles des accès logiques. En cas d'attaque sur une zone spécifique, la propagation et l'impact sur les autres zones sera contrôlé et limité.

L'ensemble de l'infrastructure est géré par l'infogéreur cegedim.cloud, certifié HDS v1.1 (et en cours d'agrément SecNumCloud), offrant les garanties maximales en termes de sécurité.Notamment, la sécurité autour de la gestion des postes de travail, la traçabilité des actions des utilisateurs, le contrôle des accès physiques, la gestion des personnels limitent les possibilités d'attaques internes.

Enfin, l'anonymisation en sortie d'EDS selon les critères du G29 garantit l'impossibilité de ré-identification une fois les données livrées aux destinataires finaux.

La durée de conservation de 24 mois réduit également le risque d'attaque, ces données étant supprimées une fois le projet finalisé.

1.1.5. Gravité : Impact sur les personnes

Importante : l'impact est non négligeable car en cas d'accès illégitime aux données couplé à une ré-identification des personnes, cela pourrait pénaliser le patient que certains médicaments qu'il prend soient connues publiquement. Toutefois, cet impact est atténué par le fait que la base de données SOG HEALTH contient uniquement des données sensibles relatives à la délivrance de médicaments du patient et que ces données sont pseudnonymisées.

Chapitre VI. ETUDE D'IMPACT DES ATTEINTES POTENTIELLES A LA VIE PRIVEE

La donnée mise à disposition dans l'espace projet n'est qu'un sous-ensemble de la donnée SOG HEALTH, correspondant uniquement aux données pertinentes dans le cadre du projet

1.1.6. Vraisemblance du risque

Négligeable : la sécurité en place autour des données SOG HEALTH vise à empêcher l'accès aux personnes non autorisées.

Le chiffrement des données permet de protéger les données et de les rendre très difficilement utilisables en cas de cyber attaque.

Le cloisonnement limite grandement la portée d'action de l'attaquant.

La journalisation permet de tracer les actions des acteurs en cas de malveillance en interne.

L'accès aux données par un tiers non autorisé est peu vraisemblable car l'hébergeur/ infogérant contrôlent qui accède aux données. Les accès sont donnés exclusivement aux personnes qui réalisent les traitements. Dans le cas des données de santé, ces personnes sont exclusivement des collaborateurs CLINITYX BY GERS DATA et ont signé une charte informatique, une charte de confidentialité et ont suivi les e-learning obligatoires. Ils connaissent les risques encourus en cas d'actions malveillantes volontaires.

Les mesures de sécurité rendent très limitée la possibilité d'une cyberattaque. L'ensemble des mesures mises en place par l'hébergeur/infogérant visent à empêcher une telle action.

Dans l'éventualité d'un accès, le préjudice pour les personnes restera limité en l'absence de réidentification, dont la vraisemblance est limitée par le cloisonnement des données, par la pseudonymisation des données et par le nombre de patients inclus : moins de 0,01% de la population totale française par an, rendant les possibilités de réidentification quasiment improbable – d'autant que l'attaquant doit avoir en sa possession des données directement identifiantes et des informations communes aux deux jeux de données détenues, scénario pour laquelle la vraisemblance est peu probable, et les moyens considérés comme démesurés pour parvenir à réidentifier les patients.

L'EDS ne contient pas de données directement identifiantes et CLINITYX BY GERS DATA ne dispose pas de telles données.

L'anonymisation des données sera garantie en sortie d'EDS, rendant la réidentification des patients et prescripteurs impossibles.

1.2. Modification non désirée des données

1.2.1. Principales sources de risque

- Cybercriminel (attaque par rançongiciel),
- Utilisateurs internes (volonté de nuire à son employeur, manipulation des données pour fausser des résultats),
- Concurrence (sabotage, altération des données pour compromettre les résultats des études ou nuire à la réputation de Clinityx by GERS DATA),
- Activiste idéologique (s'opposer à des projets de recherche, démontrer une faille de sécurité dans la plateforme),
- Accident sur les data centers, erreur de manipulation (bugs et défauts de conception dans les traitements), défaillance matérielle (pannes matérielles telles que défaillances de disques durs, pannes de serveur).

1.2.2. Principales menaces

- Altération volontaire des données par un acteur externe (usurpation d'un compte, compromission d'un poste, brèche de sécurité dans la plateforme, introduction d'un virus informatique) ou par un utilisateur (corruption, pression),
- Dégât physique sur les supports de données,
- Erreur de manipulation sur les données,
- Altération des données à la suite de la mise à jour d'une application.

1.2.3. Principaux impacts potentiels

Sans impact sur les personnes concernées dans la mesure où le traitement ne sert pas à leur prise en charge.

1.2.4. Principales mesures réduisant la gravité et la vraisemblance

Tous les flux sont sécurisés, et la donnée est chiffrée, rendant illisible le contenu et demandant des efforts disproportionnés à l'attaquant afin de compromettre leur intégrité en cas de compromission. Par ailleurs, la durée de conservation de 24 mois dans l'espace projet, sur uniquement un sous-ensemble de la base de données SOG HEALTH, minimise grandement la gravité d'une modification non désirée des données.

Les données sont traitées dans des environnements cloisonnés selon le plus haut niveau de sécurité en vigueur, avec des règles strictes de contrôles des accès logiques. En cas d'attaque sur une zone spécifique, la propagation et l'impact sur les autres zones sera contrôlé et limité.

Des sauvegardes sont régulièrement effectuées.

L'ensemble de l'infrastructure est géré par l'infogéreur cegedim.cloud, certifié HDS v1.1, offrant les garanties maximales en termes de sécurité.

Notamment, la sécurité autour de la gestion des postes de travail, la traçabilité des actions des utilisateurs, le contrôle des accès physiques, la gestion des personnels limitent les possibilités d'attaques internes.

Les sources de risques non humaines sont sécurisées par des mesures fortes en termes d'éloignement et de la protection des sources de risques non humaines, notamment dans la lutte contre le feu, des risques électriques et de la gestion de la température et de l'hygrométrie autour des data centers.

1.2.5. Gravité : impact sur les personnes

Négligeable : Sans impact car le traitement ne sert pas à la prise en charge des personnes concernées.

Par ailleurs, les mesures de sauvegarde entourant le traitement de la donnée permettent de restituer la donnée à son état avant modification/altération en cas de réussite de l'attaque.

1.2.6. Vraisemblance du risque

Négligeable : les mesures mises en place protègent les données.

La sécurité en place autour des données SOG HEALTH vise à empêcher l'accès aux personnes non autorisées.

Le chiffrement des données permet de protéger les données et de les rendre très difficilement modifiables en cas de cyber attaque.

Le cloisonnement limite grandement la portée d'action de l'attaquant.

Si les données de l'espace projets sont corrompues par un attaquant, elles peuvent être réextraites à partir de la base SOG HEALTH, d'autant que les actes malveillants sont détectés rapidement par la traçabilité et la journalisation des actions des utilisateurs.

Le contrôle des accès permet de limiter les accès aux données aux personnes responsables et sensibilisées aux risques de modification des données.

L'accès aux données par un tiers non autorisé est peu vraisemblable car l'hébergeur/ infogérant contrôlent qui accède aux données. Les accès sont donnés exclusivement aux personnes qui réalisent les traitements. Dans le cas des données de santé, ces personnes sont exclusivement des collaborateurs CLINITYX BY GERS DATA et ont signé une charte informatique, une charte de confidentialité et ont suivi les e-learning obligatoires. Ils connaissent les risques encourus en cas d'actions malveillantes volontaires.

Les mesures de sécurité rendent très limitée la possibilité d'une cyberattaque. L'ensemble des mesures mises en place par l'hébergeur/infogérant visent à empêcher une telle action.

La sécurisation autour des sources de risque empêche la dégradation des données.

1.3. Disparition des données

1.3.1. Principales sources de risque

- Cybercriminel (attaque avec un virus informatique),
- Ransomware Operators (obtenir des paiements en échange de la restauration de la donnée),
- Utilisateurs internes (volonté de nuire à son employeur),
- Concurrence (supprimer les données pour obtenir un avantage stratégique),
- Activiste idéologique (s'opposer à des projets de recherche, démontrer une faille de sécurité dans la plateforme),
- Accident sur les data centers, erreur de manipulation (bugs et défauts de conception dans les traitements), défaillance matérielle (pannes matérielles telles que défaillances de disques durs, pannes de serveur).

1.3.2. Principales menaces

- Destruction volontaire des données par un acteur externe (usurpation d'un compte, compromission d'un poste, introduction d'un virus informatique) ou par un utilisateur (corruption, pression)
- Dégât physique sur les supports de données,
- Brèche de sécurité dans la plateforme,
- Erreur de manipulation sur les données,
- Suppression des données à la suite de la mise à jour d'une application.

1.3.3. Principaux impacts potentiels

Négligeable : Sans impact sur les personnes concernées dans la mesure où le traitement ne sert pas à leur prise en charge.

1.3.4. Principales mesures réduisant la gravité et la vraisemblance

Des sauvegardes sont régulièrement effectuées.

L'ensemble de l'infrastructure est géré par l'infogéreur cegedim.cloud, certifié HDS v1.1, offrant les garanties maximales en termes de sécurité.

Notamment, la sécurité autour de la gestion des postes de travail, la traçabilité des actions des utilisateurs, le contrôle des accès physiques, la gestion des personnels limitent les possibilités d'attaques internes.

Les sources de risques non humaines sont sécurisées par des mesures fortes en termes d'éloignement et la protection des sources de risques non humaines, notamment dans la lutte

contre le feu, les risques électriques et la gestion de la température et de l'hygrométrie autour des data centers.

1.3.5. Gravité : impact sur les personnes

Négligeable : le traitement des personnes concernées ne sert pas à leur prise en charge

1.3.6. Vraisemblance du risque

Négligeable : les mesures mises en place concernant la protection de cyberattaques, ainsi que la sécurisation d'accès aux données rendent la vraisemblance d'une disparition des données SOG HEALTH très faible.

Si les données de l'espace projets sont corrompues par un attaquant, elles peuvent être réextraites à partir de la base SOG HEALTH, d'autant que les actes malveillants sont détectés rapidement par la traçabilité et la journalisation des actions des utilisateurs.

Le contrôle des accès permet de limiter les accès aux données aux personnes responsables et sensibilisées aux risques de disparition des données.

L'accès aux données par un tiers non autorisé est peu vraisemblable car l'hébergeur/ infogérant contrôle qui accède aux données. Les accès sont donnés exclusivement aux personnes qui réalisent les traitements. Dans le cas des données de santé, ces personnes sont exclusivement des collaborateurs CLINITYX BY GERS DATA et ont signé une charte informatique, une charte de confidentialité et ont suivi les e-learning obligatoires. Ils connaissent les risques encourus en cas d'actions malveillantes volontaires.

Les mesures de sécurité rendent très limitée la possibilité d'une cyberattaque. L'ensemble des mesures mises en place par l'hébergeur/infogérant visent à empêcher une telle action.

La sécurisation autour des sources de risque empêche la disparition des données.

VI.2. Évaluation des risques

2.1. Accès illégitime à des données

Acceptable/ Améliorable ?	**Acceptable**
Gravité résiduelle	**Importante**
Vraisemblance résiduelle	**Négligeable**

2.2. Modification non désirée des données

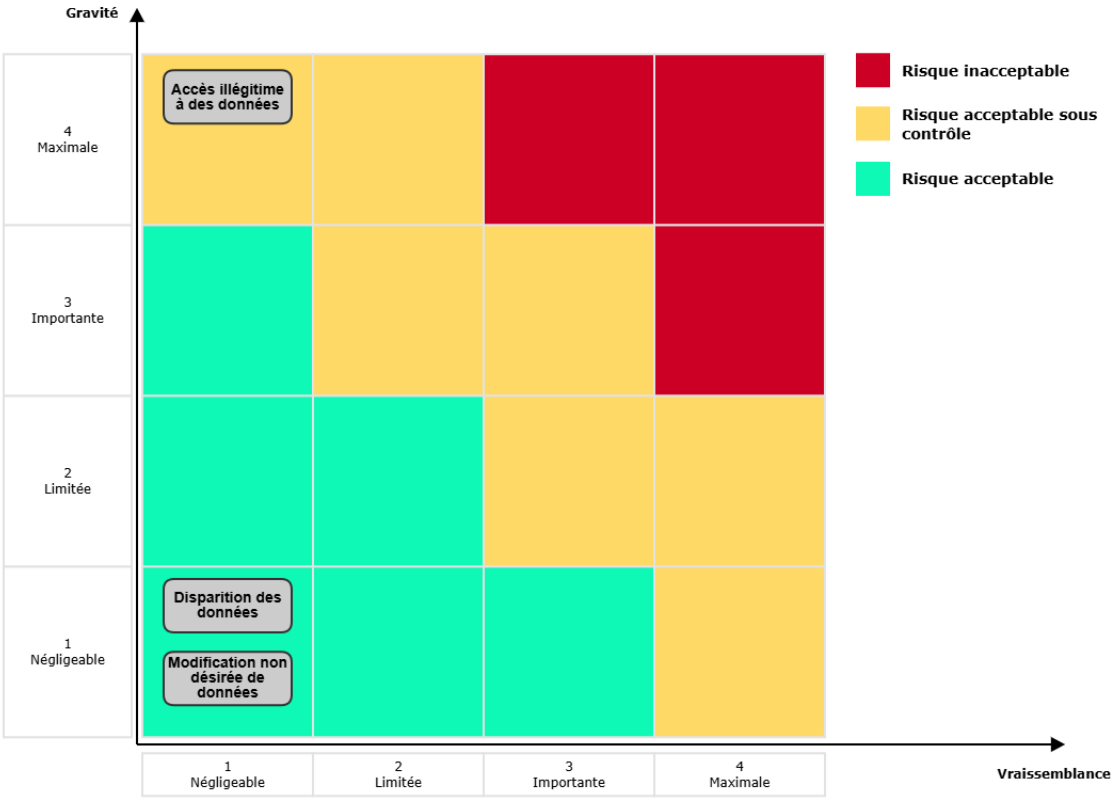
Acceptable/ Améliorable ?	**Acceptable**
Gravité résiduelle	**Négligeable**

Vraisemblance résiduelle	**Négligeable**

2.3. Disparition des données

Acceptable/ Améliorable ?	**Acceptable**
Mesures correctives	NA
Gravité résiduelle	**Négligeable**
Vraisemblance résiduelle	**Négligeable**

2.4. Cartographie des risques



Chapitre VII. MODELES UTILES A LA VALIDATION DU PIA

VII.1. Préparation des éléments utiles à la validation

Légende				
Symbole :	●●●	●○○	○●○	○○●
Signification :	Non applicable	Insatisfaisant	Amélioration prévue	Satisfaisant

1.1. Elaboration de la synthèse relative à la conformité au RGPD des mesures permettant de respecter les principes fondamentaux

Mesures permettant de respecter les principes fondamentaux	Evaluation
Mesures garantissant la proportionnalité et la nécessité du traitement	
Finalités : déterminées, explicites et légitimes	○○●
Fondement : licéité du traitement, interdiction du détournement de finalité	○○●
Minimisation des données : adéquates, pertinentes et limitées	○○●
Qualité des données : exactes et tenues à jour	○○●
Durées de conservation : limitées	○○●
Mesures protectrices des droits des personnes des personnes concernées	
Information des personnes concernées (traitement loyal et transparent)	○○●
Recueil du consentement	●●●
Exercice des droits d'accès et à la portabilité	●●●
Exercice des droits de rectification et d'effacement	●●●
Exercice des droits de limitation du traitement et d'opposition	●●●
Sous-traitance : identifiée et contractualisée	○○●
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	○○●

1.2. Elaboration de la synthèse relative à la conformité aux bonnes pratiques des mesures contribuant à traiter les risques liés à la sécurité des données

Mesures contribuant à traiter les risques liés à la sécurité des données	Evaluation
Mesures portant spécifiquement sur les données du traitement	

Chapitre VII. MODELES UTILES A LA VALIDATION DU PIA

Chiffrement	○○●
Anonymisation	○○●
Cloisonnement des données (par rapport au reste du système d'information)	○○●
Contrôle des accès logiques des utilisateurs	○○●
Traçabilité (journalisation)	○○●
Contrôle d'intégrité	○○●
Archivage	○○●
Sécurité des documents papier	●●●
Mesures générales de sécurité du système dans lequel le traitement est mis en œuvre	
Sécurité de l'exploitation	○○●
Lutte contre les logiciels malveillants	○○●
Gestion des postes de travail	○○●
Sécurité des sites web	●●●
Sauvegardes	○○●
Maintenance	○○●
Sécurité des canaux informatiques (réseaux)	○○●
Surveillance	○○●
Contrôle d'accès physique	○○●
Sécurité des matériels	○○●
Éloignement des sources de risques	○○●
Protection contre les sources de risques non humaines	○○●
Mesures organisationnelles (gouvernance)	
Organisation	○○●
Politique (gestion des règles)	○○●
Gestion des risques	○○●
Gestion des projets	○○●
Gestion des incidents et des violations de données	○○●
Gestion des personnels	○○●
Relations avec les tiers	○○●
Supervision	○○●

1.3. Formalisation du conseil de la personne en charge des aspects « Informatique et libertés »

Le 20/12/2025/ , le délégué à la protection des données de Valneva France SAS a rendu l'avis suivant concernant la conformité du traitement et le PIA mené :

Avis favorable.

NICOLAS ARVIS

NICOLAS ARVIS (Dec 20, 2025 17:16:53 GMT+1)

[Nom et Signature]

Le 19/12/2025/ , le délégué à la protection des données Clinityx by GERS DATA a rendu l'avis suivant concernant la conformité du traitement et le PIA mené :

Avis favorable.

Laurene Gantzer

Laurene Gantzer

[Nom et Signature]

VII.2. Validation formelle

Le 20/12/2025/ , Nicolas Arvis de Valneva France SAS valide le PIA du traitement, au vu du PIA mené,

NICOLAS ARVIS

NICOLAS ARVIS (Dec 20, 2025 17:16:53 GMT+1)

[Nom et Signature]

Le 22/12//2025/ , Nicolas Glattde Clinityx by GERS DATA valide le PIA du traitement, au vu du PIA mené,

NICOLAS GLATT

NICOLAS GLATT

NICOLAS GLATT (Dec 22, 2025 08:20:38 GMT+1)

[Nom et Signature]

AIPD_SogHealth_PROJETS _Valneva_2010 (002)

Final Audit Report 2025-12-22

Created:	2025-12-19
By:	AURELIE HERVE (aurelie.herve@gers-sas.fr)
Status:	Signed
Transaction ID:	CBJCHBCAABAAq_1PLL0RocTi9fx7jhQHbBbQzuZNaVXi

"AIPD_SogHealth_PROJETS _Valneva_2010 (002)" History

Document created by AURELIE HERVE (aurelie.herve@gers-sas.fr)
2025-12-19 - 1:06:03 PM GMT

Document emailed to NICOLAS ARVIS (nicolas.arvis@valneva.com) for signature
2025-12-19 - 1:06:08 PM GMT

Document emailed to NICOLAS GLATT (nicolas.glatt@clinityx.com) for signature
2025-12-19 - 1:06:09 PM GMT

Document emailed to LAURENE GANTZER (laurene.gantzer@gers-sas.fr) for signature
2025-12-19 - 1:06:09 PM GMT

Email viewed by LAURENE GANTZER (laurene.gantzer@gers-sas.fr)
2025-12-19 - 2:37:53 PM GMT

Document signing delegated to Laurene Gantzer (laurene.gantzer@cegedim.com) by LAURENE GANTZER (laurene.gantzer@gers-sas.fr)
2025-12-19 - 2:37:56 PM GMT

Document e-signed by Laurene Gantzer (laurene.gantzer@cegedim.com)
Signature Date: 2025-12-19 - 2:38:21 PM GMT - Time Source: server

Email viewed by NICOLAS ARVIS (nicolas.arvis@valneva.com)
2025-12-20 - 3:42:57 PM GMT

Document e-signed by NICOLAS ARVIS (nicolas.arvis@valneva.com)
Signature Date: 2025-12-20 - 4:16:53 PM GMT - Time Source: server

Email viewed by NICOLAS GLATT (nicolas.glatt@clinityx.com)
2025-12-22 - 7:20:02 AM GMT

Document e-signed by NICOLAS GLATT (nicolas.glatt@clinityx.com)

Signature Date: 2025-12-22 - 7:20:38 AM GMT - Time Source: server

Agreement completed.

2025-12-22 - 7:20:38 AM GMT