Evaluation

Contexte

Cette section vous permet d'obtenir une vision claire du(des) traitement(s) de données à caractère personnel considéré(s).

VUE D'ENSEMBLE

Cette partie vous permet d'identifier et de présenter l'objet de l'étude.

EN ATTENTE DE VALIDATION

L'évaluation de cette partie est terminée et en attente de validation finale de l'analyse. Si vous souhaitez modifier les évaluations, il faut annuler la demande de validation.

Quel est le traitement qui fait l'objet de l'étude ?

Le traitement de données mis en œuvre par le Conseil national de l'Ordre des pharmaciens (ci-après « CNOP ») a pour finalité la gestion de l'application numérique « Dossier Pharma » qui permet aux usagers (ci-après « l'Usager ») de gérer leurs données liées à leurs traitements médicamenteux, d'avoir accès à des informations liées à la vaccination, à des rappels de prise médicamenteuse et à des informations générales sur la santé. L'application permet également un accès au Dossier Pharmaceutique (ci-après « DP ») pour ceux qui en sont bénéficiaires.

0 commentaire(s)

25/06/2025

Commenter

Quelles sont les responsabilités liées au traitement ?

Le responsable de traitement est le Conseil national de l'Ordre des pharmaciens (CNOP).

Le sous-traitant est la société Docaposte, hébergeur certifié hébergeur de données de santé (HDS), qui héberge les données de la base "Dossier Pharma".

0 commentaire(s)

17/06/2025

Commenter

Quels sont les référentiels applicables ?

- Référentiel de certification HDS (https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification)
- Référentiel INS (https://esante.gouv.fr/securite/identifiant-national-de-sante)
- Référentiel national d'identitovigilance (https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance)
- Référentiels de sécurité et d'interopérabilité (https://esante.gouv.fr/securite/pgssi-s/espace-de-publication)

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger

Acceptable

03/07/2025

Partie évaluée, en attente de la validation finale

Tous les champs doivent être remplis

Annuler la demande de validation

Données, processus et supports »

Évaluation

Contexte

Cette section vous permet d'obtenir une vision claire du(des) traitement(s) de données à caractère personnel considéré(s).

DONNÉES, PROCESSUS ET SUPPORTS

Cette partie vous permet de délimiter et décrire le traitement considéré de manière détaillée.

EN ATTENTE DE VALIDATION

L'évaluation de cette partie est terminée et en attente de validation finale de l'analyse. Si vous souhaitez modifier les évaluations, il faut annuler la demande de validation.

Quelles sont les données traitées ?

Les catégories de données à caractère personnel que le CNOP est amené à collecter et traiter dans le cadre de la mise en œuvre de Dossier Pharma sont les suivantes :

- des données administratives (identité) telles que décrites ci-dessous;
- des données de santé notamment celles du DP, listées à l'article R.1111-23 du code de la santé publique ;
- des données permettant de tracer tout accès au profil Dossier Pharma de l'Usager.

Ces données sont collectées lors de la création du compte Dossier Pharma.

Le détail de ces données est décrit ci-dessous :

Donnée	Description
SUB_FRANCECONNECT	Identifiant technique du compte dans France Connect Cet identifiant permet de s'identifier, il est donné après une connexion réussie à France Connect+
EMAIL	Email du compte accès patient, transmis par le serveur de l'application « Dossier Pharma » Cet email est lié à la connexion à France Connect+ via l'Identité Numérique de La Poste ou France Identité et est enregistré lors de cette connexion
NOM	Nom de famille de naissance.
PRENOMS	Prénoms séparés par des espaces.
GENRE	Sexe M ou F

Les données d'identité suivantes sont utilisées par le CNOP pour associer un compte « Dossier Pharma » et un DP mais elles ne sont pas conservées.

Réconciliation Identités Dossier Pharma et DP

Prénoms de naissance
Nom de naissance
Date de naissance
Sexe
Lieu de naissance

0 commentaire(s)

25/06/2025

Commenter

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

La création d'un compte Dossier Pharma est possible deux façons :

- **Création du compte et authentification via FranceConnect+ :**

Pour utiliser ce service, il est nécessaire d'avoir un compte actif, accessible via FranceConnect+, de l'Identité Numérique de la Poste ou de France Identité. Le service de l'Identité Numérique de la Poste est ouvert aux français majeurs possédant une pièce d'identité française éligible en cours de validité, un smartphone et un n° de mobile français ou d'une liste restreinte de pays. Il est également ouvert à tous les détenteurs d'un titre de séjour français qui possèdent un numéro de sécurité sociale français et dont la durée de validité est supérieure ou égale à cinq (5) ans. Le service France Identité, quant à lui, est ouvert aux français majeurs disposant du nouveau format de la carte d'identité.

Les informations ci-dessus sur les conditions d'éligibilité aux services de FranceConnect+, de L'Identité Numérique de La Poste et de France Identité sont seulement indicatives.

À noter que le compte Dossier Pharma et le compte Identité Numérique sont deux comptes différents.

L'enrôlement à Dossier Pharma permet de créer son compte Dossier Pharma.

Les étapes sont :

1. ouvrir l'application Dossier Pharma, et cliquez sur *« Créer son compte»* puis *« Je crée mon compte via FranceConnect+ »* ;
2. suivre le mode opératoire proposé puis cliquer "activer mon compte via Franceconnect+"
3. quand la page de choix du fournisseur d'identités de FranceConnect+ s'affiche, veuillez choisir l'Identité Numérique de La Poste ou France Identité ;
4. ensuite, il convient de s'authentifier avec le compte Identité Numérique de La Poste ou France Identité ;
5. après l'authentification avec France Connect + et l'Identité Numérique de La Poste ou France Identité, l'Usager est renvoyé vers Dossier Pharma, pour initialiser son compte Dossier Pharma. L'Usage doit :

   - renseigner son adresse de courrier électronique ;
   - enregistrer sa clé de sécurité (WebAuthn). Pour ce faire, il convient d'utiliser un nom descriptif lors de l'enregistrement de la clé.

Ce principe repose sur la comparaison des données d'identité qui figurent et sont utilisées par FranceConnect+ et des traits d'identité qualifiés associés à l'INS et peuplés dans le serveur du DP. A la création du compte du patient, la vérification de l'identité de l'utilisateur est déléguée à FranceConnect+ et à l'Identité Numérique de La Poste et à France Identité qui sont des fournisseurs d'identité numérique de niveau substantiel

Après la vérification d'identité, un compte IDP Pro (fournisseur d'identité de Docaposte) est créé pour permettre notamment la sécurisation des accès ultérieurs de l'utilisateur sur un appareil mobile.

En cas de succès de la recherche (1 seul DP est trouvé au regard des données d'identité utilisées) le processus d'enrôlement est réussi, en conséquence, le DP est appairé avec le compte « Accès patient ».

- **Création du compte avec confirmation de l'identité par adresse électronique**

Ce processus s'appuie sur une authentification de l'utilisateur grâce aux informations collectées par le pharmacien en officine en face à face.

Les étapes sont :

1. ouvrir l'application Dossier Pharma, et cliquez sur *« Créer son compte»* puis *« Je crée mon compte avec mon adresse de messagerie»* ;
2. l'Usager saisit dans l'application des informations d'identité (son numéro d'inscription au répertoire « NIR » / Numéro de série de sa Carte Vitale / sa Date de naissance). Ces informations sont transmises au serveur du DP qui vérifie si un seul dossier pharmaceutique est trouvé pour ces éléments d'identité. Si cela est le cas, le CNOP vérifie la présence d'une adresse électronique de messagerie collectée par un pharmacien d'officine. Si un seul DP est trouvé et dispose d'une adresse de messagerie, un compte Accès patient inactif est créé. Ce dernier est en attente de la confirmation par la saisie d'un code temporaire transmis à l'adresse de messagerie enregistrée dans le Serveur DP.
3. l'Usager saisit dans l'application le code à usage unique temporaire («code OTP ») reçu à l'adresse de messagerie collectée par le pharmacien d'officine. Si le code saisi est correct, le compte IDP Pro (fournisseur d'identité de Docaposte)est actif ainsi que le compte Dossier Pharma qui est dès lors appairé avec le DP.

Dans les deux cas, une fois que le compte Dossier Pharma est créé, l'Usager est renvoyé vers la page d'accueil de Dossier Pharma. S'il s'agit de la première connexion, Dossier Pharma demande à l'Usager son consentement pour collecter et traiter ses données personnelles conformément aux stipulations de la politique de confidentialité disponible à l'adresse URL suivante : https://app.dossierpharma.fr/public-static-files/docs/protection_des_donnees_dossier_pharma.html . Si l'Usager donne son consentement, le serveur Accès Patient et le serveur Dossier Pharmaceutique Central tentent, en arrière-plan, de retrouver le DP correspondant au compte de l'Usager concerné : il s'agit du processus d'appairage.

La suppression d'un compte Dossier Pharma

L'Usager a le droit de supprimer son compte Dossier Pharma, à tout moment, directement depuis l'application mobile « Dossier Pharma ».

Cette action supprime le compte Dossier Pharma de l'Usager.

Cette action ne supprime pas :

- le compte de l'Usager auprès d'un fournisseur d'identités externe (par exemple, l'Identité Numérique de La Poste ou France Identité) ;
- le DP de l'Usager.

Pour supprimer le compte Dossier Pharma :

1. l'Usager se connecte à Dossier Pharma avec son compte Usager ;
2. l'Usager clique sur « Mon compte et mes droits > Mes démarches > Supprimer mon compte », et confirme la suppression.

0 commentaire(s)

25/06/2025

Commenter

Quels sont les supports des données ?

Les données de Dossier Pharma sont gérées sur support électronique seulement sur les serveurs de l'hébergeur certifié de données de santé Docaposte.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Acceptable

03/07/2025

Partie évaluée, en attente de la validation finale

Tous les champs doivent être remplis

Annuler la demande de validation

« Vue d'ensemble

Proportionnalité et nécessité »

Évaluation

Principes fondamentaux

Cette section vous permet de bâtir le dispositif de conformité aux principes de protection de la vie privée.

PROPORTIONNALITÉ ET NÉCESSITÉ

Cette partie vous permet de démontrer que vous mettez en œuvre les moyens nécessaires pour permettre aux personnes concernées d'exercer leurs droits.

EN ATTENTE DE VALIDATION

L'évaluation de cette partie est terminée et en attente de validation finale de l'analyse. Si vous souhaitez modifier les évaluations, il faut annuler la demande de validation.

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

L'application "Dossier Pharma" a pour finalité de permettre à chaque Usager qui le souhaite d'être associé au suivi de ses informations médicamenteuses, en particulier :

- en lui permettant d'accéder directement aux données de son DP mis en œuvre par le CNOP conformément à l'article L. 4231-2 du code de la santé publique (accès aux dispensations médicamenteuses, aux dispensations vaccinales et au calendrier vaccinal),
- en lui permettant d'exercer ses droits en ligne (gérer son compte « Dossier Pharma », visualiser les traces des accès effectués sur le DP, supprimer son DP ou se mettre sur liste d'opposition),
- en lui permettant d'améliorer l'observance (programmer des rappels de prises de médicaments),
- en facilitant l'accompagnement des aidants (permettre de donner l'accès à son DP ou de programmer des rappels de prise à un tiers),
- en facilitant l'accès aux traitements (faciliter l'accès aux informations relatives à une officine, visualiser les officines, les hôpitaux et les laboratoires à proximité).

Ces finalités sont déterminées, explicites et légitimes.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

La base légale du traitement de données et la condition qui permet le traitement de ses données de santé est le consentement de l'Usager, en application des articles

6-1-a 9-2-a du RGPD.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

A partir du traitement ainsi mis en œuvre par le CNOP, l'Usager peut :

- créer son compte sur l'application « Dossier Pharma » ;
- publier, visionner, et/ou commenter des contenus disponibles sur l'application « Dossier Pharma » ;
- modifier les informations contenues sur l'application « Dossier Pharma » ;
- contacter le CNOP par tout moyen de communication mis à sa disposition tel que le téléphone, le courrier électronique etc. ;
- naviguer sur l'application « Dossier Pharma » par l'intermédiaire de cookies ou technologies similaires.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Les données sont-elles exactes et tenues à jour ?

Les données relatives à l'identité du bénéficiaire de l'assurance maladie sont mises à jour conformément aux mises à jour effectuées sur la carte Vitale du bénéficiaire ou dans les bases utilisées par les téléservices INSi de l'Assurance maladie.

Les données relatives à l'Usager qui utilise France Connect+ sont gérés par le fournisseur d'identité qu'il sélectionne au moment de son authentification : l'Identité numérique de La Poste ou France Identité.

Les données relatives aux dispensations et aux traces d'intervention du DP sont mises à jour à chaque nouvelle dispensation réalisée dans les officines ou les pharmacies à usage intérieur raccordées au Serveur central DP et régulièrement supprimées.

Les données relatives aux coordonnées de l'Usager (adresse de messagerie) et aux actions réalisées sur l'application Dossier Pharma (rappel de prise par exemple) sont gérées directement par l'Usager lui-même dans l'application.

Les données relatives aux traces d'accès et d'utilisation du compte Dossier Pharma sont mises à jour à chaque action de l'Usager et régulièrement supprimées.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Quelle est la durée de conservation des données ?

Le CNOP conserve les données à caractère personnel de la façon suivante.

Pour les données relatives au compte Usager : jusqu'à la suppression du compte Usager ou 36 mois après le dernier accès au compte.

La suppression du compte « Dossier Pharma » entraîne l'effacement définitif et immédiat des données relatives au compte.

Pour les données communiquées via les demandes de contact : le temps nécessaire à la gestion de la demande

Pour les données transmises lors de la mise en œuvre d'un droit concédé par la Réglementation applicable en matière de Données Personnelles : le temps nécessaire au traitement de la demande.

Clôturer le compte "Dossier Pharma", ne supprime pas le contenu du DP.

Toutefois, à l'issue des délais précités, les données à caractère personnel collectées et traitées pourront être archivées au-delà des durées prévues (i) en cas de procédure contentieuse afin de permettre d'établir la réalité des faits litigieux ; et/ou (ii) pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales dans le seul but de permettre, en tant que besoins, la mise à disposition de ces données à l'autorité judiciaire.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Partie évaluée, en attente de la validation finale

Tous les champs doivent être remplis

Annuler la demande de validation

« Données, processus et supports

Mesures protectrices des droits »

Principes fondamentaux

Évaluation

Cette section vous permet de bâtir le dispositif de conformité aux principes de protection de la vie privée.

MESURES PROTECTRICES DES DROITS

Cette partie vous permet de démontrer que vous mettez en œuvre les moyens nécessaires pour permettre aux personnes concernées d'exercer leurs droits.

EN ATTENTE DE VALIDATION

L'évaluation de cette partie est terminée et en attente de validation finale de l'analyse. Si vous souhaitez modifier les évaluations, il faut annuler la demande de validation.

Comment les personnes concernées sont-elles informées à propos du traitement ?

Après l'installation, au premier lancement de l'application, l'Usager doit valider les conditions générales d'utilisation de l'application (CGU). Il peut télécharger les CGU. À chaque mise à jour de ces CGU, cette validation est à nouveau demandée à l'Usager. À défaut de validation, l'application se ferme et ne peut être utilisée par l'Usager.

Après la création de son compte, pour l'appairage avec le DP, l'Usager doit valider la politique de protection des données personnelles. À défaut de cette validation, l'appairage avec son DP ne sera pas effectué et l'utilisation de l'application sera limitée aux fonctionnalités n'utilisant pas de données personnelles, particulièrement ses données de santé. Seules les données d'identité relatives à son compte Dossier Pharma sont alors enregistrées dans la base Dossier Pharma. L'Usager peut changer d'avis et accepter ou refuser la politique de protection des données personnelles a posteriori dans l'application dans le module « Mon compte et mes droits ». À chaque mise à jour de la politique de protection des données personnelles, cette validation est à nouveau demandée à l'Usager.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Le consentement de l'Usager est requis deux fois :

- pour la création de son Dossier Pharma dans la mesure où il constitue la base légale du traitement de données lié à l'application ; à cet effet il coche une case après avoir pris connaissance de la politique de confidentialité qui respecte les exigences d'information de l'article 13 du RGPD ;

- pour l'acceptation des CGU de l'application Dossier Pharma.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

L'Usager peut accéder directement aux données contenues dans son compte "Dossier Pharma" en utilisant ses moyens d'identification et d'authentification. Une fois connecté, il aura accès directement aux données stockées dans "Dossier Pharma".

Droit d'accès et droit à la portabilité : il accède directement à l'ensemble de ses données traitées dans l'application "Dossier Pharma".

Le droit à la portabilité sera assuré et permettra à l'Usager de demander la transmission de ses données vers une autre application.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit à l'effacement (droit à l'oubli) ?

L'Usager peut directement effectuer la rectification de données qu'il a lui-même saisies.

Pour les autres données, le droit de rectification et le droit à la limitation du traitement s'exercent auprès du DPO du CNOP à l'adresse mail suivante : dpo@ordre.pharmacien.fr

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit d'opposition ?

L'Usager peut lors de la clôture de leur compte "Dossier Pharma", supprimer l'intégralité de ses données liées à son compte directement dans la rubrique "Mon Compte et mes Droits" puis "Mes Démarches". A noter que supprimer le compte Dossier Pharma, ne supprime pas le DP.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Les données à caractère personnel collectées et traitées sous la responsabilité du CNOP et de son sous-traitant, la société Docaposte certifiée hébergeur de données de santé conformément aux exigences de l'article L.1111-8 du code de la santé publique pour les stricts besoins de leurs missions nécessaires au fonctionnement de l'application « Dossier Pharma ». Les données sont hébergées en France.

Dans le cadre du contrat qui les lie, les obligations du sous-traitant sont clairement définies et conformes aux exigences de l'article 28 du RGPD. Le CNOP exige ainsi que Docaposte mette en place des mesures de sécurité techniques et organisationnelles appropriées afin de garantir la confidentialité des données personnelles et un niveau de sécurité adapté au risque.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Non applicable

0 commentaire(s)

03/07/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Partie évaluée, en attente de la validation finale

Tous les champs doivent être remplis

Annuler la demande de validation

« Proportionnalité et nécessité

Mesures existantes ou prévues »

Évaluation

Risques

Cette section vous permet d'apprécier les risques sur la vie privée, compte tenu des mesures existantes ou prévues.

MESURES EXISTANTES OU PRÉVUES

Cette partie vous permet de recenser les mesures (existantes ou prévues) contribuant à la sécurité des données.

EN ATTENTE DE VALIDATION

L'évaluation de cette partie est terminée et en attente de validation finale de l'analyse. Si vous souhaitez modifier les évaluations, il faut annuler la demande de validation.

Contrôle des accès logiques

Seuls les Usagers disposant d'un compte Dossier pharma peuvent utiliser l'application. La création d'un compte Dossier Pharma se fait soit après authentification via France Connect+ et l'Identité Numérique de La Poste ou France Identité soit par l'adresse email collectée par le pharmacien d'officine et associé au DP du patient (avec son INS qualifié). La création d'une clé WebAuthn sur l'appareil mobile par l'Usager est géré par l'IDP Pro.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Chiffrement

L'accès à l'application est entièrement en HTTPS pour que le contenu des flux qui transitent ne puisse pas être lu par des tiers non autorisés.

Pour éviter que des applications tierces puissent faire appel aux web services à destination de l'application mobile et puissent nuire au bon fonctionnement des applications, ou accéder à des données normalement destinées à l'application mobile, seule l'application mobile est autorisée à dialoguer avec les Web services. Pour s'en assurer, les appels effectués depuis l'application mobile contiennent une clé unique qui identifie l'application. Les appels émis sans clé valide sont systématiquement rejetés.

De plus, l'application utilise un mécanisme d'épinglage de certificats (SSL Pinning), qui permet de sécuriser la communication avec le serveur et éviter les attaques de type MITM (Man In The Middle), qui consistent à intercepter la communication entre l'application et le serveur.

Une partie des données à caractère personnel sont chiffrées en DB avec l'algorithme de chiffrement AES-256-GCM. Les clés ainsi que les opérations de chiffrement / déchiffrement sont effectuées par des serveurs HSM du bastion HDS de DOCAPOSTE.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Identification

Pour s'authentifier, l'Usager a deux choix :

- Authentification via FranceConnect+ : seuls les fournisseurs d'identité d'un niveau eIDAS substantiel ou élevé sont compris dans le périmètre (l'Identité Numérique de la Poste ou France Identité).

  Si le patient n'a plus de clé secrète WebAuthn enregistrée dans son compte, l'IDP Pro le demandera d'en enregistrer une nouvelle après l'authentification avec FranceConnect+.

- Authentification avec le compte IDP Pro : dans ce cas, l'utilisateur doit renseigner son login et s'authentifier en utilisant son smartphone avec WebAuthn.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Sécurité physique

Des mesures de protection contre les risques d'intrusion et de contrôle physique des accès aux locaux, aux équipements et aux outils sont mises en place par l'hébergeur des données (Docaposte) y compris vis-à-vis des prestataires externes (nettoyage, livraisons...).

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Traçabilité

Toutes les interventions réalisées par les utilisateurs habilités sont tracées, conformément aux exigences de la certification hébergeur de données de santé.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Pas d'extraction permanente

Il n'est pas possible d'extraire de façon permanente les données individuelles du serveur Dossier Pharma.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Superviser la protection de la vie privée

L'hébergeur a l'obligation de réaliser régulièrement des contrôles de sécurité, de conformité et de qualité des applications qu'il héberge.

Il doit également permettre au CNOP d'effectuer des audits sur les applications mises en production.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Contrat de sous-traitance

Le CNOP confie l'hébergement de l'ensemble des bases du système d'exploitation de l'application Dossier Pharma à Docaposte, hébergeur certifié de données de santé conformément à l'article L. 1111-8 du code de la santé publique.
Le contrat conclu entre le CNOP et Docaposte est conforme aux dispositions légales, en ce compris les dispositions de l'article R. 1111-11 du code de la santé publique.
L'article 28 du RGPD est également pris en compte.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Durée de conservation limitée

Les données sont régulièrement effacées conformément aux durées de conservation des données décrites dans la présente AIPD.

Des procédures de contrôle ont été mises en place afin de s'assurer de la bonne réalisation des opérations de suppression définitive des données.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Exercice des droits de limitation du traitement et d'opposition

L'Usager peut lors de la clôture de leur compte "Dossier Pharma", supprimer l'intégralité de ses données liées à son compte directement dans la rubrique "Mon Compte et mes Droits" puis "Mes Démarches". A noter que supprimer le compte Dossier Pharma, ne supprime pas le DP.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Exercice des droits de rectification et d'effacement

L'Usager peut directement effectuer la rectification de données qu'il a lui-même saisies.

Pour les autres données, le droit de rectification et le droit à la limitation du traitement s'exercent auprès du DPO du CNOP à l'adresse mail suivante : dpo@ordre.pharmacien.fr.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Gérer les incidents de sécurité et les violations de données

Une procédure de gestion des incidents de sécurité ou de violations des données est mise en œuvre au sein du CNOP d'une part, au sein de Docaposte, hébergeur de Dossier Pharma d'autre part.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Gestion des personnels

Des formations régulières sur la mise en œuvre du RGPD et la protection des données personnelles sont réalisées régulièrement auprès de l'ensemble des équipes de Docaposte et du CNOP travaillant sur l'application Dossier Pharma.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Intégrer la protection de la vie privée dans les projets

Tout projet d'évolution d'un traitement existant ou développement d'un nouveau projet prévoit systématiquement une analyse au regard de la protection des données personnelles.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Gérer les risques

Une procédure de gestion des risques a été rédigée dans le cadre du nouveau contrat d'hébergement de l'application Dossier Pharma. Cette procédure est référencée en pièce jointe à la présente AIPD.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Lutte contre les logiciels malveillants

Docaposte, en tant qu'hébergeur certifié de données de santé, répond aux critères de lutte contre les logiciels malveillants.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Maintenance

Docaposte, en tant qu'hébergeur certifié de données de santé, met en œuvre les mesures propres à limiter les risques de violation ou d'altération des données lors des opérations de maintenance.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Organisation de la politique de protection de la vie privée

Le CNOP a désigné un DPO. Ce dernier est sollicité dès lors qu'une question relative à l'application Dossier Pharma et à la protection des données personnelles se pose selon une procédure arrêtée avec l'Ordre. Le DPO du CNOP participe au comité conformité trimestriel mis en place par le CNOP spécifiquement sur le suivi des dossiers liés à l'application Dossier Pharma.

Docaposte a désigné un DPO. Ce dernier participe au comité de pilotage opérationnel trimestriel organisé par le CNOP et est sollicité pour toutes les questions touchant aux données personnelles.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Protection contre les sources de risques non humaines

Docaposte, en tant qu'hébergeur certifié de données de santé, répond aux critères de protection contre les risques humains et non humains d'altération des données.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Gestion des tiers accédant aux données.

Docaposte, en tant qu'hébergeur certifié de données de santé, répond aux critères de gestion des tiers accédant aux données.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Sauvegarde des données

Les bases de données de l'application Dossier Pharma sont dupliquées de manière actif-actif sur deux sites. L'ensemble des équipements est redondé afin de garantir la disponibilité des données.

Une procédure de sauvegarde des données a été mise en place : celle-ci prévoit des sauvegardes complètes et des sauvegardes incrémentales permettant de reconstituer l'ensemble des données en cas de perte d'un site.

Enfin, un troisième site de secours a été mis en place dans le cadre du contrat d'hébergement conclu en 2020 avec Docaposte.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Sécurisation de l'exploitation

Docaposte, en tant qu'hébergeur certifié de données de santé, répond aux critères de sécurité de l'exploitation des données dans le cadre de l'application Dossier Pharma.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Sécurisation des canaux informatiques

Docaposte, en tant qu'hébergeur certifié de données de santé, répond aux exigences de sécurité des canaux informatiques utilisés dans le cadre de l'application Dossier Pharma.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Partie évaluée, en attente de la validation finale

Tous les champs doivent être remplis

Annuler la demande de validation

« Mesures protectrices des droits

Accès illégitime à des données »

Évaluation

Risques

Cette section vous permet d'apprécier les risques sur la vie privée, compte tenu des mesures existantes ou prévues.

ACCÈS ILLÉGITIME À DES DONNÉES

Analysez les causes et conséquences d'un accès illégitime à des données, et estimez sa gravité et sa vraisemblance.

EN ATTENTE DE VALIDATION

L'évaluation de cette partie est terminée et en attente de validation finale de l'analyse. Si vous souhaitez modifier les évaluations, il faut annuler la demande de validation.

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Divulgation de données de santé de l'Usager

Divulgation des données relatives aux professionnel...

Saisissez les impacts potentiels

0 commentaire(s)

25/06/2025

Commenter

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Hacking des serveurs de Docaposte Hacking de l'appareil mobile de l'Usager

Anomalie dans les serveurs de Docaposte ou sur l'ap...

Mauvaise sécurisation par l'Usager de son appareil ...

Saisissez les menaces

0 commentaire(s)

25/06/2025

Commenter

Quelles sources de risques pourraient-elles en être à l'origine ?

Un tiers malveillant L'hébergeur/intégrateur de l'application Dossier phar...

L'Usager lui-même

Saisissez les sources de risques

0 commentaire(s)

25/06/2025

Commenter

Quelles sont les mesures initiales, parmi celles identifiées, qui contribuent à traiter le risque ?

Chiffrement Contrôle des accès logiques Identification

Pas d'extraction permanente Superviser la protection de la vie privée

Sécurité physique Durée de conservation limitée

Lutte contre les logiciels malveillants Sécurisation des canaux informatiques

Traçabilité Gérer les incidents de sécurité et les violations de d… Maintenance

Cliquez ici pour sélectionner les mesures contribuant à traiter ce risque.

0 commentaire(s)

17/06/2025

Commenter

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Les données de dispensations hébergées dans le cadre du DP et accessibles grâce à l'application Dossier Pharma peuvent donner des indications sur l'état de santé d'une personne. La divulgation de ces informations à un tiers ou le fait de les rendre publiques peuvent avoir des impacts sur l'état de santé ou l'état psychique de la personne, voire l'empêcher de réaliser certaines actions.

0 commentaire(s)

17/06/2025

Commenter

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Au regard des mesures de sécurité mises en œuvre par Docaposte, hébergeur certifié de données de santé, l'accès illégitime aux données au niveau des serveurs de Docaposte est négligeable.

S'agissant de l'appareil mobile de l'usager, les systèmes de sécurité proposés par les appareils mobiles (faceID, clé WebAuthn...), le risque d'accès illégitime reste très limité.

0 commentaire(s)

17/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Partie évaluée, en attente de la validation finale

Tous les champs doivent être remplis

Annuler la demande de validation

« Mesures existantes ou prévues

Modification non désirées de données »

Évaluation

Risques

Cette section vous permet d'apprécier les risques sur la vie privée, compte tenu des mesures existantes ou prévues.

MODIFICATION NON DÉSIRÉES DE DONNÉES

Analysez les causes et conséquences d'une modification non désirée de données, et estimez sa gravité et sa vraisemblance.

EN ATTENTE DE VALIDATION

L'évaluation de cette partie est terminée et en attente de validation finale de l'analyse. Si vous souhaitez modifier les évaluations, il faut annuler la demande de validation.

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Défaut d'observance dans la prise de ses traitement...

Saisissez les impacts potentiels

0 commentaire(s)

17/06/2025

Commenter

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Hacking des serveurs de Docaposte Hacking de l'appareil mobile de l'Usager

Anomalie dans les serveurs de Docaposte ou sur l'ap...

Mauvaise sécurisation par l'Usager de son appareil ...

Saisissez les menaces

0 commentaire(s)

25/06/2025

Commenter

Quelles sources de risques pourraient-elles en être à l'origine ?

L'hébergeur/intégrateur de l'application Dossier phar... Un tiers malveillant

L'Usager lui-même

Saisissez les sources de risques

0 commentaire(s)

25/06/2025

Commenter

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Sécurité physique Contrôle des accès logiques

Superviser la protection de la vie privée Identification Traçabilité

Exercice des droits de rectification et d'effacement

Gérer les incidents de sécurité et les violations de d… Gérer les risques

Sauvegarde des données Lutte contre les logiciels malveillants

Sécurisation de l'exploitation

Cliquez ici pour sélectionner les mesures contribuant à traiter ce risque.

0 commentaire(s)

17/06/2025

Commenter

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Une atteinte à l'intégrité des données peut contribuer à un mauvais suivi par l'Usager des prises de ses traitements.

0 commentaire(s)

25/06/2025

Commenter

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Au regard des mesures de sécurité mises en œuvre par Docaposte, hébergeur certifié de données de santé, la modification non désirée de données au niveau des serveurs de Docaposte est négligeable.

S'agissant de l'appareil mobile de l'Usager, les systèmes de sécurité proposés par les appareils mobiles (faceID, clé WebAuthn...), la modification non désirée de

données par l'Usager ou un tiers malveillant reste là aussi négligeable.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Partie évaluée, en attente de la validation finale

Tous les champs doivent être remplis

Annuler la demande de validation

« Accès illégitime à des données

Disparition de données »

Évaluation

Risques

Cette section vous permet d'apprécier les risques sur la vie privée, compte tenu des mesures existantes ou prévues.

DISPARITION DE DONNÉES

Analysez les causes et conséquences d'une disparition de données, et estimez sa gravité et sa vraisemblance.

EN ATTENTE DE VALIDATION

L'évaluation de cette partie est terminée et en attente de validation finale de l'analyse. Si vous souhaitez modifier les évaluations, il faut annuler la demande de validation.

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Défaut d'observance dans la prise de ses traitement...

Saisissez les impacts potentiels

0 commentaire(s)

17/06/2025

Commenter

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Hacking des serveurs de Docaposte

Anomalie dans les serveurs de Docaposte ou sur l'ap...

Hacking de l'appareil mobile de l'Usager

Mauvaise sécurisation par l'Usager de son appareil ...

Saisissez les menaces

0 commentaire(s)

25/06/2025

Commenter

Quelles sources de risques pourraient-elles en être à l'origine ?

L'hébergeur/intégrateur de l'application Dossier phar... Un tiers malveillant

L'Usager lui-même

Saisissez les sources de risques

0 commentaire(s)

25/06/2025

Commenter

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Superviser la protection de la vie privée Sécurité physique

Contrôle des accès logiques Traçabilité Gérer les risques

Lutte contre les logiciels malveillants

Protection contre les sources de risques non humai…

Gestion des tiers accédant aux données. Sauvegarde des données

Sécurisation de l'exploitation

Cliquez ici pour sélectionner les mesures contribuant à traiter ce risque.

0 commentaire(s)

07/11/2024

Commenter

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Une disparition des données peut contribuer à un mauvais suivi par l'Usager des prises de ses traitements.

0 commentaire(s)

25/06/2025

Commenter

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

(Non définie) Négligeable Limitée Importante Maximale

Au regard des mesures de sécurité mises en œuvre par Docaposte, hébergeur certifié de données de santé, la disparition de données au niveau des serveurs de Docaposte est négligeable.

S’agissant de l'appareil mobile de l'Usager, les systèmes de sécurité proposés par les appareils mobiles (faceID, clé WebAuthn...), la disparition de données par l'Usager ou un tiers malveillant reste là aussi négligeable.

0 commentaire(s)

25/06/2025

Commenter

Évaluation

À corriger | Améliorable | Acceptable

03/07/2025

Partie évaluée, en attente de la validation finale

Tous les champs doivent être remplis

Annuler la demande de validation

« Modification non désirées de données

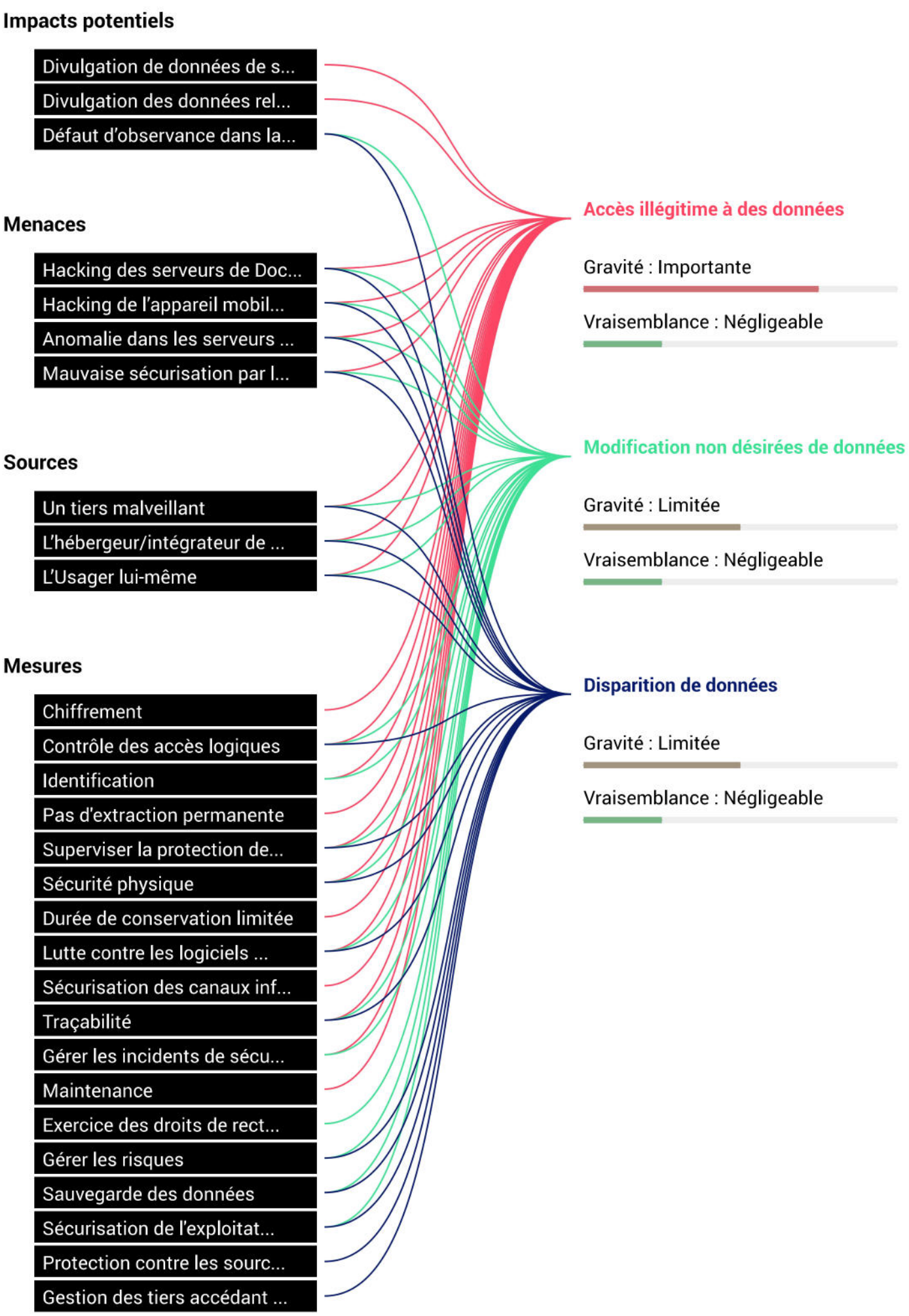
Vue d'ensemble des risques »

Risques

Cette section vous permet d'apprécier les risques sur la vie privée, compte tenu des mesures existantes ou prévues.

VUE D'ENSEMBLE DES RISQUES

Cette visualisation vous permet d'avoir une vue globale et synthétique de l'action des mesures sur les composants des risques qu'elles contribuent à traiter.

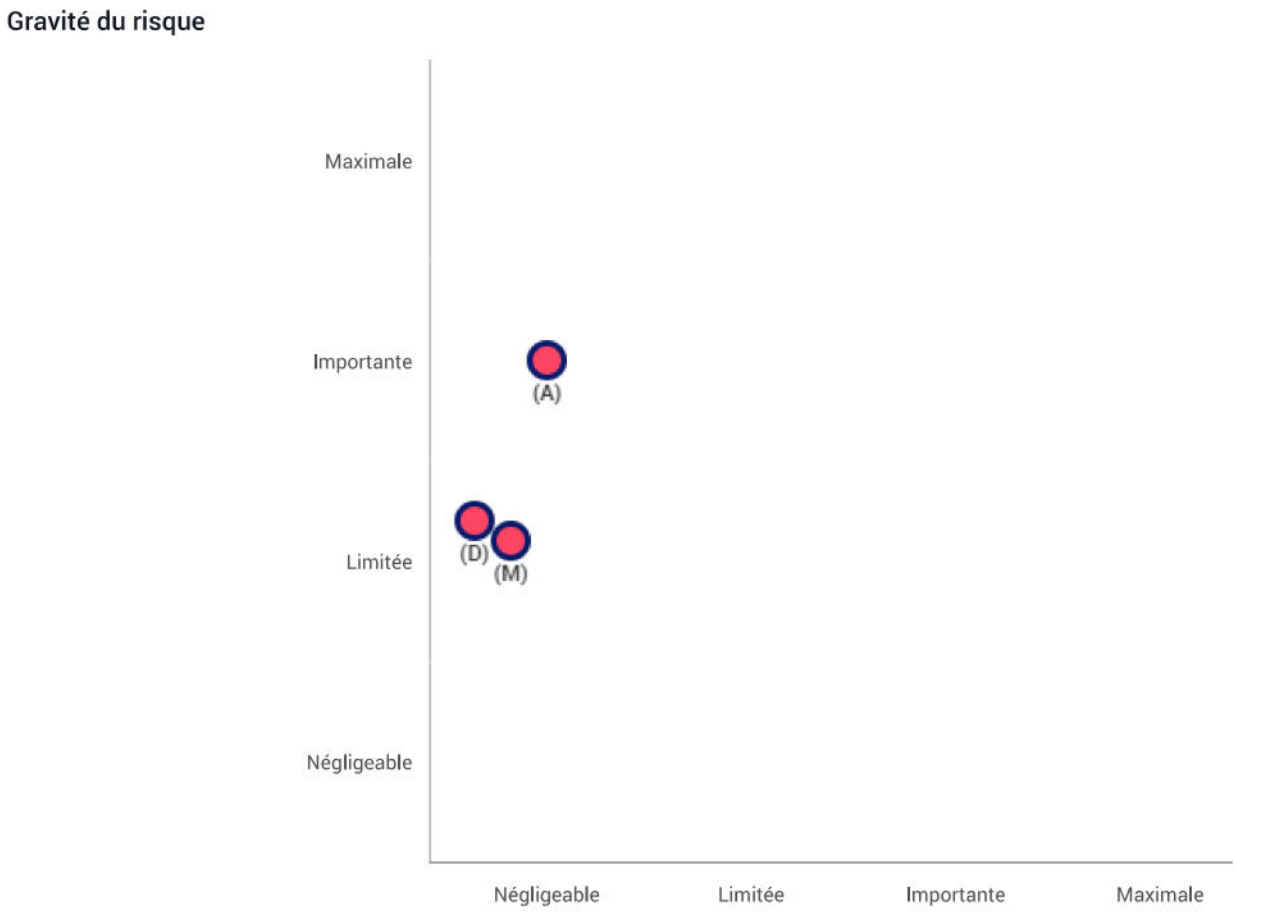

Impacts potentiels
Divulgation de données de s...
Divulgation des données rel...
Défaut d'observance dans la...
Menaces
Hacking des serveurs de Doc...
Hacking de l'appareil mobil...
Anomalie dans les serveurs ...
Mauvaise sécurisation par l...
Sources
Un tiers malveillant
L'hébergeur/intégrateur de ...
L'Usager lui-même
Mesures
Chiffrement
Contrôle des accès logiques
Identification
Pas d'extraction permanente
Superviser la protection de...
Sécurité physique
Durée de conservation limitée
Lutte contre les logiciels ...
Sécurisation des canaux inf...
Traçabilité
Gérer les incidents de sécu...
Maintenance
Exercice des droits de rect...
Gérer les risques
Sauvegarde des données
Sécurisation de l'exploitat...
Protection contre les sourc...
Gestion des tiers accédant ...
Accès illégitime à des données
Gravité : Importante
Vraisemblance : Négligeable
Modification non désirées de données
Gravité : Limitée
Vraisemblance : Négligeable
Disparition de données
Gravité : Limitée
Vraisemblance : Négligeable

Validation

Cette section vous permet de préparer et de formaliser la validation du PIA.

CARTOGRAPHIE DES RISQUES

Cette visualisation vous permet de comparer le positionnement des risques entre eux, avant et après application des mesures complémentaires.



- Mesures prévues ou existantes
- Avec les mesures correctives mises en oeuvre
- (A)ccès illégitime à des données
- (M)odification non désirée de données
- (D)isparition de données

17/06/2025

« Vue d'ensemble des risques

Plan d'action »

Validation

Cette section vous permet de préparer et de formaliser la validation du PIA.

PLAN D'ACTION

Planifiez en détail la mise en œuvre des mesures complémentaires déterminées au cours du PIA. Cette partie est automatiquement mise à jour en fonction des évaluations faites de chaque élément composant l'analyse d'impact.

Vue d'ensemble

Principes fondamentaux

Finalités
Fondement
Données adéquates
Données exactes
Durée de conservation
Information des personnes
Recueil du consentement
Droit d'accès et à la portabilité
Droit de rectification et d'effacement
Droit de limitation et d'opposition
Sous-traitance
Transferts

Mesures existantes ou prévues

Contrôle des accès logiques
Chiffrement
Identification
Sécurité physique
Traçabilité

Risques

Accès illégitime à des données
Modification non désirée de données
Disparition de données

Mesures Améliorables
Mesures Acceptables

Principes fondamentaux

Aucun plan d'action enregistré.

Mesures existantes ou prévues

Aucun plan d'action enregistré.

Risques

Aucun plan d'action enregistré.

« Cartographie des risques

Avis du DPD et des personnes concernées »

Validation

Cette section vous permet de préparer et de formaliser la validation du PIA.

Édition

AVIS DU DPD ET DES PERSONNES CONCERNÉES

Présentez le conseil de la personne en charge des aspects informatique et libertés (délégué à la protection des données s'il existe). Présentez l'avis des personnes concernées ou de leurs représentants.

Avis du DPD

Le DPO du CNOP considere(nt) que :

- ✔ Le traitement pourrait être mis en oeuvre.
- ○ Le traitement ne devrait pas être mis en oeuvre.

Précisez les raisons de votre choix

Avis des personnes concernées

- ✔ L'avis des personnes concernées a été demandé.
- ○ L'avis des personnes concernées n'a pas été demandé.

Nom(s) de la(des) pers(considère(nt) que :

- ○ Le traitement pourrait être mis en oeuvre.
- ○ Le traitement ne devrait pas être mis en oeuvre.

Décrivez comment les avis ont été collectés et quelle en est l'analyse. Dans le cas où les avis n'ont pas été recherchés, en préciser les raisons.