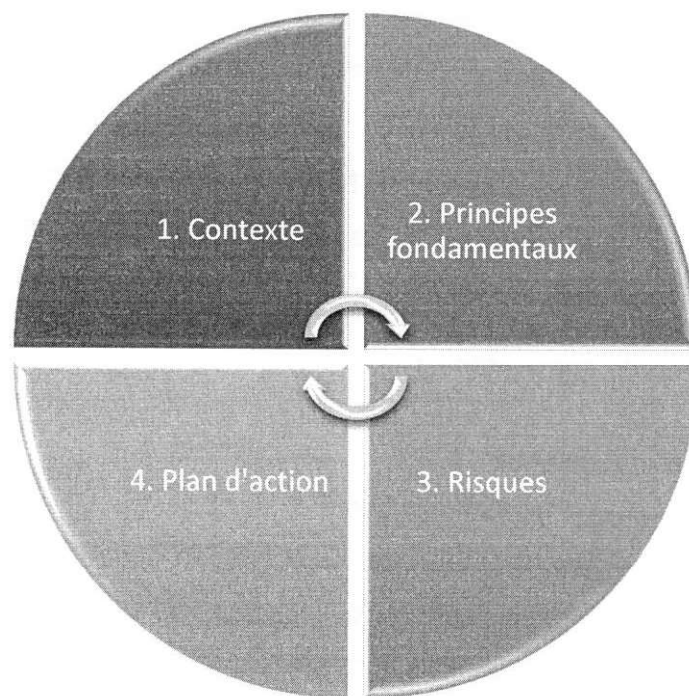



PIA – NOVA PMI

ANALYSE D'IMPACT RELATIVE A L'APPLICATION NOVA
UTILISEE DANS LE SERVICE DE LA PROTECTION MATERNELLE
ET INFANTILE (PMI) – MAJ DU PIA INITIAL



Saisine :	 Délégue à la protection des données
Evaluation :	
Validation :	
Date de création : 21 août 2019	
Date de mise à jour : 2 février 2023	

Responsable de traitement : Direction de l'enfance et de la famille – Service de la protection maternelle et infantile

PARTIE 1 – CONTEXTE

1.1. VUE D'ENSEMBLE

Quel est le traitement qui fait l'objet d'une étude ?

Gestion du dossier médical, paramédical et administratif d'un usager par le service PMI via l'application NOVA.

Quelles sont les responsabilités liées au traitement ?

Responsable de traitement : Direction de l'enfance et de la famille

Par délégation : Service de la protection maternelle et infantile

Sous-traitants :

- Wordline/SANTEOS : éditeur du logiciel NOVA et hébergeur des données de santé
- Acteur FSE : interfacé pour permettre la télétransmission des feuilles de soin électroniques à l'Assurance maladie.

Quels sont les référentiels applicables ?

- RGPD
- Loi informatique et libertés de 1978
- Référentiel CNIL sur les données de santé
- Certification HDS de SANTEOS en date du 1^{er} juin 2019 renouvelée le 22 mai 2022 (cf. <https://santeos.com/fr/home/blog/2022/octobre/worldline-santeos-renouvelle-sa-certification-hebergeur-de-donnees-de-sante-en-allant-au-dela-des-exigences.html>)

Code de la santé publique : articles L2111-1, L2112-1 à L2112-10 (service de PMI), L2122-1 à L2122-5 (examens de prévention durant et après la grossesse), L2132-1 à L2132-5 (carnet de santé et examen obligatoire), R2112-8

-
- Code de la sécurité sociale : L.162-32

1.2. DONNEES, PROCESSUS ET SUPPORTS

Quelles sont les données traitées ?

Les données recueillies concernent les usagers des centres de PMI et de planification familiale:

- données administratives des usagers
- données socio-économiques
- déterminants de santé (environnement de vie, addictions ..)

- données de santé (antécédents médicaux de l'utilisateur dans les autres services, vaccins, données des consultations médicales ...)
- bilan de santé en école maternelle
- facturation des actes réalisés
- indicateurs épidémiologiques et de santé publique

Les données concernent également les professionnels des centres :

- traces de navigation / consultation / modifications des dossiers usagers
- données d'activité (nombre de consultations réalisées par ex.) dans l'infocentre

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

Les données sont saisies dans les centres de PMI et de planification. Le dossier médical est créé par le service à son arrivée dans un centre. A tout moment, l'utilisateur peut demander à accéder ou récupérer son dossier médical.

Un dossier peut être rattaché à un autre centre après consentement de l'utilisateur, en cas de déménagement par exemple.

Les données peuvent être analysées sur les sites locaux et aux bureaux centraux (bureau épidémiologique et la mission d'aide au pilotage) du service de PMI.

Concernant la fin de vie des données : un processus a été vu avec la DSA (cf. Durée de conservation plus bas).

Un export des utilisateurs est réalisé au moins 1 fois par semestre.

Quels sont les supports des données ?

Support principal : logiciel NOVA.

Les données numériques sont hébergées sur les serveurs de SANTEOS-Worldline situé en EU.

Certaines données, exportées, peuvent être stockées sur les ordinateurs des utilisateurs professionnels de PMI. Ces exports sont limités à certains profils utilisateurs.

Les extractions de ces données pourront être stockées sur un coffre-fort numérique PMI (en projet - à construire avec le RSSI). Une solution mobile est utilisée pour les bilans de santé maternelle et VAD (ordinateurs portables). Deux technologies sont mises en œuvre:

- mode connecté : fonctionnement normal
- mode déconnecté : données chiffrées stockées en local

Cf. cahier de spécifications de la solution mobile de SANTEOS précisant les mesures de sécurité adaptées (chiffrement, sécurisation des transmissions, ...) en PJ de ce PIA, dans le fond de dossier.

Des consultations ont lieu dans des sites non départementaux (PMI conventionnés) donc les utilisateurs peuvent utiliser des ordinateurs non départementaux qui sont soumis aux règles de sécurité informatique locales.

PARTIE 2 – PRINCIPES FONDAMENTAUX

2.1. PROPORTIONNALITE ET NECESSITE

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

Les traitements cités ci-avant (fondement de la mission d'intérêt public) ont pour finalité d'assurer des consultations médicales et des actions de prévention médico-sociale en faveur des futurs parents, des femmes enceintes, des enfants de moins de 6 ans et répondent à des missions réglementaires définies par les articles du Code de Santé Publique (CSP) (art. L 2111-1 et L2112-2). Ces missions de la PMI sont organisées par le président du conseil départemental. Elles peuvent être exercées en régie directe ou confiées à un établissement de santé, à une commune ou encore à une association (article L.2112-4 du CSP). En outre, le logiciel NOVA participe à la modernisation des outils du service, et est mieux adapté à sa volumétrie.

Les traitements relatifs aux données épidémiologiques, de santé publique et d'activité du service permettent d'une part de décrire l'état de santé de la population usagère de la PMI et d'autre part de piloter l'activité du service. Ces traitements répondent aux articles L 2132-2, L 2132-3 et R 2112-8 du CSP.

Les consultations de PMI sont facturées à la CPAM - via le logiciel "ActeurFSE" embarqué dans NOVA - pour la réalisation et la télétransmission de feuilles de soins électroniques des actes médicaux. Une convention fixe les conditions de participation des organismes d'assurance maladie au fonctionnement du service de PMI et les conditions de remboursement des actes médicaux prévus dans le Code de santé publique (art L.2112-7) et du Code de la sécurité sociale (art L.162-32).

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

Mission d'intérêt public (vu avec la DAJIA en concertation avec les trois services utilisant le logiciel NOVA dans leurs domaines respectifs).

Le service départemental de protection maternelle et infantile exerce les missions qui lui sont dévolues par les articles L. 2112-1 et L. 2112-2 en organisant notamment, soit directement, soit par voie de convention les consultations, visites à domicile et autres actions médico-sociales, individuelles ou collectives, de promotion de la santé maternelle et infantile.

Une convention établie entre le département et la CPAM permet la prise en charge financière des actes facturés par les professionnels de santé des centres de PMI (cf. Code de la santé publique (art L 2112-7) et du Code de la sécurité sociale (art L 162-32)).

Les traitements relatifs aux données épidémiologiques, de santé publique et d'activité du service permettent d'une part de décrire l'état de santé de la population usagère de la PMI et d'autre part de piloter l'activité du service. Ces traitements répondent aux articles L 2132-2, L.2132-3 et R.2112-8 du CSP.

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) ?

Les professionnels de PMI collectent les informations administratives, psycho-sociales et médicales nécessaires au bon suivi des usagers.

On distingue:

d'une part, les données courantes :

- état-civil : éléments nécessaires pour la constitution du dossier administratif
- vie personnelle : éléments nécessaires à la prise en charge de l'usager,
- vie professionnelle : éléments strictement nécessaires à la prise en charge du patient
- données de connexion des professionnels

d'autre part, les données de santé :

- NIR : remboursements CPAM
- les données de santé, dont des données relatives à la vie sexuelle (dans le cadre des consultations de planification et entretiens de conseil conjugal).

Il existe des champs libres dans le logiciel (exemple : anamnèse pour les consultations médicales), réservés aux professionnels ayant entretenu ou réalisé la consultation. Le contenu de ces champs libres n'est pas exploitable statistiquement (aucune remontée dans l'infocentre) et des règles de bonnes pratiques sont exposées aux professionnels en formation utilisateur.

De plus, il y a un cloisonnement des données entre les 3 services (CSS, SPAS, PMI) : seule la fiche identité administrative est partagée pour éviter les doublons.

Les données sont-elles exactes et tenues à jour ?

Les données sont recueillies sur la base du déclaratif (pas de vérification) et des examens médicaux.

Elles sont mises à jour en fonction des déclarations des usagers (ces mises à jour sont historiées dans le logiciel) et en fonction du suivi médico-social.

Seule la donnée du NIR peut faire l'objet d'une vérification (et mise à jour en projet).

A venir : formation du métier pour sensibiliser sur la nécessité de mettre à jour les données.

Quelle est la durée de conservation des données ?

La Direction du service des archives a été consultée (cf. tableau de gestion des archives de la DSA et Art. R. 1112-7 du CSP).

Le délai de conservation prévu pour les dossiers médicaux des établissements de santé est de :

- 20 ans à compter de la date de la dernière consultation du patient
- Si le patient est mineur et que ce délai de 20 ans expire avant son 28e anniversaire, la conservation des informations le concernant doit être prolongée jusqu'à cette date

La Direction du service des archives du Département confirme :

- la durée de conservation des données telles que définie ci-dessus
- pas d'archivage des données prévu au-delà des durées de conservation prévues

2.2. MESURES PROTECTRICES DES DROITS

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

Avant le déploiement de NOVA : Une information sur l'informatisation du dossier paramédical est faite :

- par voie d'affichage à l'accueil, en salle d'attente et dans les cabinets médicaux
- par voie orale, par l'auxiliaire de puériculture étant généralement le 1er contact avec le centre de PMI. A cette occasion, l'utilisateur est informé de ses droits de manière dématérialisée sur NOVA (case cochée et nom du professionnel ayant informé l'utilisateur) pour chaque service fréquenté par l'utilisateur.

Dans la mention relative aux droits du patient sur ses données personnelles, le contact du DPO sera indiqué.

A la date du déploiement dans les centres de PMI:

- les personnes sont informées oralement lors de la création de leur dossier NOVA. L'utilisateur est informé de ses droits à cet égard (droit d'accès, modification, effacement, limitation et opposition) → mise à jour à venir du texte apparaissant dans le pop-up afin de respecter les mentions RGPD.

NB: sans cette information, la saisie des données médicales n'est pas possible.

Des affiches figureront dans les salles d'attente et à l'accueil des PMI comportant une mention sur le droit d'accès et rectification des données personnelles → après vérification, ses affiches sont bien affichées au 31 janvier 2023.

Enfin, une note de la DEF destinée aux usagers est en cours d'édition.

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

Pas de consentement

Comment les personnes concernées peuvent-elles exercer leurs droit d'accès, d'information, de rectification, de limitation, d'effacement et d'opposition ?

Préalablement à toute communication, le destinataire de la demande doit vérifier l'identité du demandeur.

- Concernant le droit d'accès : l'utilisateur formalise sa demande auprès des professionnels des centres et/ou du DPO du Département de Seine Saint Denis (mail, courrier). L'accès aux données se fait, au choix du demandeur, soit par consultation sur place avec éventuellement remise de copies, soit par l'envoi des documents (si possible en recommandé avec accusé de réception).
- Concernant le droit de rectification : Le patient en fait la demande aux professionnels des centres et / ou saisi le DPO du Département de la Seine-Saint-Denis (mail, courrier). Les professionnels disposant des habilitations (référénts dans les centres ou administrateurs) procèdent aux rectifications, en respect des obligations légales (données inexactes, équivoques, incomplètes, à condition de disposer d'un motif légitime).
- Concernant le droit de limitation : Le process est similaire pour l'exercice du droit d'accès ou de rectification. L'utilisateur formalise sa demande auprès des professionnels des centres et/ou du DPO du Département de Seine Saint Denis (mail, courrier) et la limitation s'effectuera, sous réserve d'un motif légitime. Il existe par ailleurs des possibilités de limiter les données recueillies pour les patients :
 - envoi de SMS Oui/Non
 - partage du n° de téléphone : Oui/Non
 - liberté du patient dans la réponse aux items.
- Concernant le droit d'opposition : idem, l'utilisateur formalise sa demande auprès des professionnels des centres et/ou auprès du DPO. Néanmoins, l'utilisateur doit mettre en avant des raisons tenant à sa situation particulière pour effacer ses données. De plus, le département peut refuser cette demande si motif légitime (en l'occurrence, le dossier de l'utilisateur ne pourra être traité sans que ses données ne soient présentes sur NOVA).

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

Worldline est hébergeur de données de santé et a reçu une certification HDS. Son obligation d'hébergement est définie.

Le document précisant les conditions d'hébergement et de maintenance concernant Worldline a été reçu en juin 2019 par le DPO. Cette certification a été renouvelée en mai 2022 (vérifier si le RSSI dispose du document).

Un marché public définit les obligations de Santeos et Santeos emploie un sous-traitant Atlantide pour le logiciel "ActeurFSE".

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

Pas de transfert hors UE.

PARTIE 3 – RISQUES

3.1. MESURES EXISTANTES OU PREVUES

Le détail des mesures se trouve dans les documentations techniques produites.

Chiffrement

Document : NOE-001-Mémoire méthodologique et technique 3.5.1. Chiffrement des données

Santeos présente ci-dessous les règles générales et les exceptions principales.

La liste présentée ici n'est pas exhaustive et la phase de spécifications détaillées reviendra, point par point, sur le dictionnaire des informations du S.I et sur les règles de chiffrement applicables et appliquées en fonction de la sensibilité des données d'une part, et de

- Toutes les pièces jointes (courriers entrant ou sortant) sont chiffrées, avec la clé de l'utilisateur

Anonymisation

- Le passage d'un dossier nominatif en dossier anonyme est possible.
- Il est possible de créer un dossier anonyme
- Les données de l'infocentre (traitements statistiques) sont d'emblée anonymes.

Document : NOE-017- Anonymisation de dossiers Nova

Pour garantir le caractère irréversible de l'anonymisation, nous proposons un mécanisme de création de dossier anonyme reprenant une partie du dossier initial et la suppression du dossier original.

Avant la validation de l'anonymisation, un message de confirmation sera affiché explicitant que les données supprimées le seront définitivement et sans récupération possible.

- Les données qui seront conservées seront basées sur le contenu des formulaires anonymisés tel qu'envoyé à l'infocentre (aucun champ alphanumérique ne sera repris):
 - Identité anonymisée
 - Formulaire
 - Antécédents
 - Données socio-économiques anonymisées
- Les autres données seront supprimées :
 - RDV
 - SMS
 - Publipostage
 - Courrier reçu et envoyés
 - Pièces Jointes
 - Observation et alertes (dossier)
 - Notes liées aux consultations
 - Liens familiaux
 - Certificats

Document : NOE-001-Mémoire méthodologique et technique

2.2.17. Infocentre

L'infocentre ne contient que des données anonymes. Pour les besoins en rapports concernant les patients ou des listes de patients, il est nécessaire de passer par NOVA au moyen de requêtes prédéfinies.

Contrôle des accès logiques

- Définition des profils utilisateurs par corps professionnels (cf fichier utilisateurs bureau Info PMI) avec droits respectifs
- Authentification : mot de passe/login

Document : NOE-001-Mémoire méthodologique et technique

3.5.3. Contrôles d'accès et traçabilité

Dans NOVA, chaque action fait l'objet d'un contrôle d'accès. Même si une action n'est pas proposée à l'utilisateur si son profil ne lui permet pas de l'exécuter, un contrôle supplémentaire est effectué côté serveur avant de « servir » une fonctionnalité. La définition des profils utilisateur et l'administration des droits par profil a été détaillé dans le chapitre décrivant les fonctionnalités de NOVA.

Comme évoqué dans le chapitre fonctionnel, toute action de l'utilisateur est tracée.

Contrôle d'intégrité

Document : PQR

6.6. Assurer la sécurité de la plateforme (analyse de risques SSI du prestataire ?)

8.3. Gestion de configuration des logiciels

8.3. Gestion de configuration des logiciels

La gestion de configuration consiste à définir et à contrôler les versions des logiciels, à gérer les modifications des éléments configurés, à enregistrer et éditer l'état de ces éléments, à enregistrer les demandes de mise en configuration, les demandes de modification (évolutif ou correctif), et à vérifier que tous ces éléments sont complets et cohérents pendant tout le cycle de vie du logiciel.

Document : NOE-001-Mémoire méthodologique et technique

3.1.3. Règle de sécurité applicables à l'hébergement

Journalisation

Document : PQGdS

13. Gestion des Incidents

Document : NOE-001-Mémoire méthodologique et technique

2.2.15.1.6. Traçabilité et historique

2.2.15.1.6. Traçabilité et historique

Toutes les actions de l'utilisateur lors d'une session sont tracées.

Archivage

Le tableau de gestion des archives a été transmis par la DSA et ajouté en PJ de ce PIA.

Document : PQP

12.2.1. Sauvegardes, sécurité, archivage

Document : NOE-001-Mémoire méthodologique et technique

2.2.16. Archivage et destruction du dossier

L'archivage des données médicales de NOVA est assuré par le Département via l'archivage des sauvegardes des données de NOVA.

La politique de durée de rétention et de stockage des archives est laissée à la discrétion du Département.

SANTEOS recommande la production d'une archive avant l'exécution des traitements de destruction de dossiers.

Sécurisation des documents papier

Les seuls documents papiers perdurant à la PMI sont les suivants :

- Compte-rendu de VAD n'ayant pas pu être réalisées dans NOVA: une fois de retour au centre, les comptes rendus sont saisis dans NOVA et sont détruits
- Résultats laboratoire, compte-rendu d'hospitalisations, courriers de confrères... : ces documents, si besoin, sont scannés et enregistrés dans NOVA. Les documents papiers sont ensuite, si besoin, remis aux usagers et ne sont pas conservés dans les centres de PMI.

Document : PQP

7.3.11. Conservation et Destruction

Gestion des postes de travail

Document : NOE-001-Mémoire méthodologique et technique

2.2.1.1. Description

3.3. Poste de travail

Sécurisation de l'exploitation

Document : PQGdS

16. Gestion des Accès

Document : NOE-001-Mémoire méthodologique et technique

3.1. Solution d'hébergement

Sauvegarde des données

Document : NOE-001-Mémoire méthodologique et technique

2.2.16. Archivage et destruction du dossier

3.1.1.4.5. Outils de supervision mis à disposition

Cloisonnement

Document : CD93-NOE-002-Cloisonnement des données médicales

Tout le document (demande de la dernière version à la DINSI)

Ajouter le fichier excel des habilitations par corps professionnels dès que finalisé et validé par la PMI.

Seules les données d'identités sont partagées dans NOVA entre les trois services, les autres données de l'utilisateur spécifique à chaque secteur d'activité sont cloisonnées par service.

Traçabilité

Document : PQGdS

10. Gestion des Déploiements et Mises en Production

13. Gestion des Incidents

16. Gestion des Accès

Document : NOE-001-Mémoire méthodologique et technique

2.2.15.1.6. Traçabilité et historique

Contrat de sous-traitance

Marché public signé avec SANTEOS, sous-traitant Atlantide et Worldline (hébergement).

Sécurisation des canaux informatiques et des matériels

Document : NOE-001-Mémoire méthodologique et technique

3.1. Solution d'hébergement

Sécurité physique

Document : NOE-001-Mémoire méthodologique et technique

3.1. Solution d'hébergement

L'hébergeur est certifié HDS, donc respect du référentiel.

Formation des agents

A venir : formation des nouveaux utilisateurs de NOVA (agents) par le biais du prestataire.

	Principaux impacts	Principales menaces	Sources de risques	Mesures	Gravité	Vraisemblance
Accès illégitime	Atteinte au secret médical Atteinte à la réputation Protection de l'enfance Diffamation donnant lieu à des représailles Syndical	Accès illégitime au dossier du patient Impression ou photocopies de dossiers d'usagers Echange de mot de passe	Source humaine interne malveillante ou accidentelle Sinistre chez SANTEOS Source humaine externe agissant de manière délibérée	Anonymisation Gestion des postes de travail Contrôle des accès logiques Journalisation Archivage Contrôle d'intégrité Sécurisation des documents papiers Sécurisation de l'exploitation Sauvegarde des données Chiffrement Contrôle des accès logiques	Avant le plan d'action : Maximale Après le plan d'action : Limitée	Avant le plan d'action : Limitée Après le plan d'action : Limitée
Modification non désirée	Défaut de prise en charge médicale Défaut de prise en charge médico-sociale	Erreur de dossier Piratage extérieur Usurpation d'identité	Source humaine interne ou externe malveillante ou accidentelle	Archivage Sécurisation des documents papiers Chiffrement Contrôle des accès logiques	Avant le plan d'action : Importante Après le plan d'action : Limitée	Avant le plan d'action : Limitée Après le plan d'action : Limitée
Disparition	Défaut de prise en charge médicale	Manipulation accidentelle Usurpation d'identité Piratage extérieur Sinistre chez l'hébergeur	Source humaine interne ou externe malveillante ou accidentelle	Contrôle des accès logiques Archivage Sécurisation de l'exploitation Sauvegarde des données Chiffrement	Avant le plan d'action : Importante Après le plan d'action : Limitée	Avant le plan d'action : Limitée Après le plan d'action : Limitée

3.2. VUE D'ENSEMBLE DES RISQUES

Impacts potentiels

Atteinte au secret médical
Atteinte à la réputation (e...
Protection de l'enfance
Diffamation donnant lieu à
Défaut de prise en charge n
Défaut de prise en charge n
Défaut de prise en charge n

Menaces

Accès illégitime au dossier
impression ou photocopies
échange de mot de passe
Des personnes présentes su
Une modification pourrait é
Piratage extérieur (données
Une personne pourrait acci
Sinistre chez l'hébergeur (...)

Sources

Source humaine interne ma
Source humaine interne acc
Sinistre chez Santéos : inc..
source humaine externe agi
Source humaine extérieure
Source naturelle (incendie,...

Mesures

Chiffrement
Anonymisation
Gestion des postes de trava
Contrôle des accès logiques
Journalisation
Archivage
Contrôle d'intégrité
Sécurisation des documents
Sécurisation de l'exploitat..
Sauvegarde des données

Accès illégitime à des données

Gravité : Maximale

Vraisemblance : Limitée

Modification non désirées de d

Gravité : Importante

Vraisemblance : Limitée

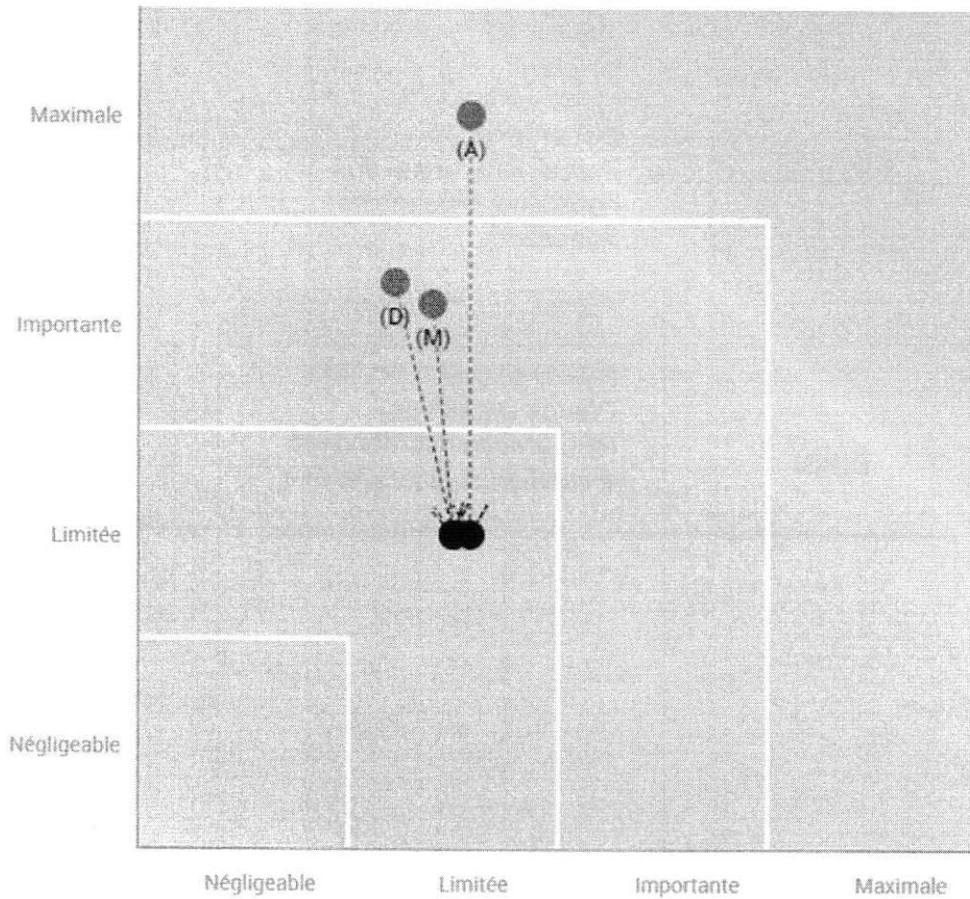
Disparition de données

Gravité : Importante

Vraisemblance : Limitée

3.3. CARTOGRAPHIE DES RISQUES

Gravité du risque



- 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

Vraisemblance du risque

PARTIE 4 – PLAN D’ACTION

Acteurs	Actions à réaliser	Date butoir
DEF/PMI	Prévoir un coffre-fort numérique bureautique pour stocker les requêtes qui pourraient être produites et stockées sur le SI Départemental	18/12/2020
	Prévoir une revue des habilitations au moins annuelle	30/06/2021
	Prévoir une formation (processus sensibilisation RGPD et cybersécurité)	
DINSI	Prévoir un test de restauration des données annuel avec le prestataire	30/03/2021

PARTIE 5 – AVIS DU DPO

Le Délégué à la protection des données (DPO) considère que le présent traitement soumis aux mesures listées dans l'analyse, peut être mis en œuvre, sous réserve de la prise en compte du plan d'action susvisé.

Le responsable de traitement accepte les mesures choisies, les éventuels risques résiduels au regard des enjeux préalablement identifiés et de l'avis des parties prenantes. Le PIA peut ainsi être validé.

NOM : MERLE

Signature Directeur ou chef
de service PMU

Par délégation Ghyslaine MERLE
Médecin Cheffe du Service
de PMI

