*Analyse d'impact relative à la protection des données (AIPD)*

# Gestion des données sanitaires au sein du Service de la Prévention et des Actions Sanitaires (SPAS)

## Avis de la DPD et des personnes concernées

Le traitement est nécessaire à l'exécution d'une mission d'intérêt public. Il doit être mis en œuvre avec les mesures de sécurité listées dans la présente et améliorées selon le plan d'action.

## Vue d'ensemble

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

Logiciel métier du SPAS (NOVA édité par Santeos-Wordline) permettant :

- gestion des RDV et planning des centres de dépistage
- dossier administratif du patient
- dossiers médicaux (IST, vaccination, psychologue/sexologue, gynécologue, buccodentaire)
- module de prescription (médicaments, examens y compris analyses biologiques)
- la télétransmission des feuilles de soins électroniques à l'assurance maladie via l'interfaçage entre le logiciel métier NOVA et un logiciel de télétransmission (Acteur FSE édité par Aatlandide)
- dossier social
- gestion des stocks et commande de médicaments
- traitements statistiques anonymisés via l'infocentre mis à disposition par l'éditeur
- export de données nominatives via des requêtes définies avec l'éditeur (ex : liste des patients suivi par un professionnel)

### Quelles sont les responsabilités liées au traitement ?

Le traitement des données est assuré par le Département de la Seine-Saint-Denis en particulier, le service de la prévention et des actions sanitaires (SPAS) de la Direction de la Prévention et de l'action sociale (DPAS).

L'hébergement des données est assuré par Santeos / WolrdLine.

### Quels sont les référentiels applicables ?

Wordline est certifié hébergeur de données de santé (certification HDS 1.1 juin 2018) certificat daté de juin 2019.

## Données, processus et supports

### Quelles sont les données traitées ?

Pour le SPAS, les données recueillies concernent les usagers des centres de dépistage :
- données administratives des patients (Etat civil, adresse, NIR,...)

- données socio-économiques (conditions d'hébergement, situation d'emploi...)
- déterminants de santé (vie sexuelle, addictions ...)
- données de santé (antécédents médicaux, données des consultations médicales incluant les demandes d'analyses biologiques et résultats...)
- données sociales

Les données concernent également les professionnels des centres :
- traces de navigation
- traces de consultation des dossiers patients
- trace de modification des dossiers patients

La fiche identité est commune aux trois services utilisant NOVA.
Elle peut contenir les données suivantes :

- Identité
  - Civilité, Nom marital, nom de naissance, Prénom, date de naissance, sexe, autres prénoms, n° sécurité sociale, lieu de naissance et n° interne NOVA. ***Les seuls champs obligatoires sont Nom de naissance, prénom, date de naissance et sexe***
- Adresse
  - les éléments types d'une adresse (n°, type de voie, nom de la voie, code postal ville,....) et la possibilité de renseigner des adresses complémentaires. Aucun champ obligatoire
- Contact
  - Possibilité de renseigner un ou plusieurs contacts avec nom, n° de téléphone,.... L'information pour recevoir des SMS est dans ce sous ensemble. Par défaut, l'information est renseignée à 'non renseignée'. Aucun champ obligatoire
- Couverture sociale
  - Existence d'une couverture sociale (nécessaire pour la facturation FSE) et information sur la CAF. Pas de champs obligatoires
- Éléments référentiels
  - N° du référentiel et N°Damoc. Ces informations sont non modifiables car renseignées automatiquement via le référentiel usager

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

Quelques précisions :

- Hébergement des données chez l'éditeur.
- Un dossier peut être rattaché à un autre centre après accord du patient.
- Un patient peut demander à accéder, obtenir son dossier médical.
- Les données sont analysées au service central du SPAS.

- la télétransmission de feuilles de soins électroniques vers l'assurance maladie s'effectue dans le cadre de la cotation des actes du bus dentaire départemental (opérationnel en janvier 2020) qui aura le statut de centre de santé (art.L6323 du Code de la Santé Publique).

## Quels sont les supports des données ?

Logiciel - serveurs

# Proportionnalité et nécessité

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

**Les finalités du traitement dans les centres de dépistage sont :**

- Organisation des consultations dans les centres de dépistage

- Suivi médical des patients

**Les finalités du traitement en externe entre notamment dans le cadre de financements obtenus pour les programmes du SPAS (CeGIDD, vaccination, bucco-dentaire, tuberculose, assurance maladie...) :**

- Transmission des données réglementaires (ARS, Santé Publique France)

- Bordereau CPAM vaccination

- Feuilles de soins électroniques

*Sous-traitant de NOVA dans le cadre de ce marché, est interfacé pour permettre la télétransmission des feuilles de soins électroniques à l'Assurance maladie

**Les finalités du traitement en interne, au service central du SPAS sont :**
- Analyses de données épidémiologiques

- Pilotage du service : analyses des données d'activité

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

***Fondement légal du traitement des données personnelles :***

**Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.**

Le Conseil Départemental de Seine-Saint-Denis est une collectivité territoriale (article 72 de la Constitution).

La loi de modernisation de l'action publique territoriale et d'affirmation des métropoles (MAPTAM) du 27 janvier 2014 et la loi portant nouvelle organisation territoriale de la République (NOTRe) du 7 août 2015 désignent le département comme **"chef de file" en matière d'aide sociale, d'autonomie des personnes et de solidarité des territoires**.

Le code de l'Action Sociale et des Familles prévoient notamment que « *Le département définit et met en œuvre la politique d'action sociale, en tenant compte des compétences confiées par la loi à l'Etat, aux autres collectivités territoriales ainsi qu'aux organismes de sécurité sociale. Il coordonne les actions menées sur son territoire qui y concourent. Il organise la participation des personnes morales de droit public et privé mentionnées à l'article L. 116-1 à la définition des orientations en matière d'action sociale et à leur mise en œuvre. » (L121-1).*

## 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) ?

Seules les données d'identité indispensables à la création du dossier (nom – prénom – date de naissance- sexe) sont obligatoires dans le logiciel. Les autres informations, tant sur l'identité que sur la situation sociale, ne sont saisies que selon les besoins.

L'appréciation des difficultés est recueillie d'abord pour évaluer la situation sociale de la personne mais aussi, le cas échéant, en vue de la sollicitation d'un dispositif réglementaire particulier.
Conformément à l'éthique et à la déontologie du travail social, les données doivent être les plus factuelles et objectives possibles, et ne sont de toutes façons notées que si elles présentent un intérêt pour l'évaluation de la situation de l'usager et les actions en sa faveur.

## Les données sont-elles exactes et tenues à jour ?

Les données sont recueillies sur la base du déclaratif lors des échanges entre professionnels des centres (secrétaires, infirmiers, médecins ...) et les patients.

Les données sont mises à jour en fonction des déclarations des patients (ces mises à jour sont historisées dans le logiciel).

## Quelle est la durée de conservation des données ?

Article R. 1112-7 du CODE DE LA SANTE PUBLIQUE

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. À l'issue de cette durée de conservation, les dossiers médicaux seront éliminés après visa de la directrice des Archives départementales.

Contrairement aux dossiers « patients» qui ont une durée de conservation assez longue, les données relatives à la prise de rendez-vous peuvent être supprimées après 2 ans et après visa de la directrice des Archives départementales.

# Mesures protectrices des droits

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

Le patient est informé de l'existence des dossiers informatiques et de leurs droits à cet égard.

**Cette information est faite :**

- Par voie d'affichage à l'accueil, en salle d'attente et dans les cabinets médicaux et dans le bus dentaire.

- Une mention figure sur l'auto-questionnaire remis au patient lors d'un premier dépistage IST en CeGIDD.

- Enfin, le patient est informé du recueil informatique de ces données, de son droit d'accès, modification et suppression lors de son premier RDV. A cette occasion, son consentement est recueilli de manière dématérialisée sur NOVA (case cochée et nom du professionnel ayant recueilli le consentement).

- En action hors-les-murs, lorsque le recueil de données se fait par papier pour une saisie ultérieure, une case permet d'indiquer que le patient a bien été informé. Des affiches sont également prévues pour les actions hors les murs.

- Le patient est en droit de ne pas répondre aux questions posées.

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

- Dans le cadre d'une prise en charge CeGIDD, le patient peut bénéficier de l'anonymat. Cette possibilité est indiquée au patient lors de son accueil dans les centres (par voie d'affichage et lors de la création du dossier par le secrétariat).

- Les personnes sont informées lors de la création de leur dossier administratif.

- Le consentement est alors recueilli oralement et enregistré sous forme informatique dans NOVA : case à cocher + nom de la personne recueillant le consentement, cette action permet la création du dossier médical.

- Sans ce consentement, la saisie des données médicales n'est pas possible.

- En cas de retrait du consentement, le logiciel prévoit la possibilité d'anonymiser le dossier patient (sont exclus les dossiers avec vaccinations ou prescriptions).

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

Le consentement n'est pas demandé dans NOVA.

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

**Concernant le droit d'accès :**

Le patient formalise sa demande auprès des professionnels des centres et/ou du DPO du Département de la 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).

Le logiciel prévoit la fonction d'impression du dossier médical avec possibilité d'impression du dossier complet ou partiel (sélection de périodes, de parties spécifiques du dossier).

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

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

Les patients ont la **possibilité de demander la rectification** de leurs données si elles sont inexactes ou incomplètes directement auprès des agents du SPAS ou auprès de la DPD.

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

L'usager peut demander aux professionnels de la circonscription en charge de son dossier à ce que ses données ne fassent plus l'objet d'un traitement durant un temps déterminé. La DPD devra en être informée.

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

Un marché public attribué à SANTEOS-WORDLINE a été signé dans lequel figure les obligations du sous-traitant.

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

Aucun transfert en dehors de l'UE.

## Mesures existantes ou prévues

### Chiffrement

Les données (contenu du dossier usager) sont chiffrées par l'éditeur.

### Anonymisation

Les fonctionnalités suivantes existent dans le logiciel NOVA :

- 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.

## Contrôle des accès logiques

Définition des profils utilisateurs par corps professionnels avec droits respectifs.

Authentification : mot de passe/login

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.

## Contrôle d'intégrité

Certification HDS

Les règles de sécurité applicables à l'hébergement sont décrites dans le Plan Assurance Qualité (PAQ) ainsi que dans le paragraphe dédié à la présentation des Data Center de Seclin.

## Journalisation

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

## Archivage

L'archivage des données médicales ou sociales 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 documents papiers sauvegardés sont les dossiers des usagers.

## Gestion des postes de travail

- Authentification AD
- Verrouillage automatique
- Ordinateur inaccessible au public
- Respect de la PSSI départementale

## Sécurisation de l'exploitation

L'exploitation est déléguée à SANTEOS-WORDLINE dans le cadre du marché.

## Sauvegarde des données

Sauvegardes journalières gérées par l'éditeur et le Département.

## Cloisonnement

Cloisonnement des données par services et profils.

## Traçabilité

Traçabilité et historique accessibles par les administrateurs de l'outil NOVA.

## Contrat de sous-traitance

Existence d'un marché public :
Santeos : intégrateur de l'application
Wordline: hébergement

## Sécurisation des canaux informatiques

Documentation éditeur conforme à la PSSI départementale.

## Sécurité physique

Datacenter sécurisé avec normes à jour.

## Lutte contre les logiciels malveillants

Installation d'un anti-virus sur tous les postes de travail

## Protection des sites web

Certificat de sécurité à jour et conforme.

## Organisation de la politique de protection de la vie privée

- Nomination d'un DPO
- Notes envoyées en 2018 sur la mise en conformité RGPD
- Conférences de sensibilisation vie privée
- Note du service social départemental
- Affiches de sensibilisation
- Nomination de relais RGPD au sein des services
- Processus de gestion des violations de données

## Gestion des personnels

Les nouveaux utilisateurs sont créés dans NOVA par les administrateurs. Les codes d'accès de ces nouveaux utilisateurs ne sont communiqués qu'après formation et remise d'un guide utilisateur.

Au départ d'un agent, les administrateurs désactivent le compte NOVA.

# Accès illégitime à des données

### Impacts :

Atteinte à la vie privée, Atteinte au secret médical, Atteinte à la réputation (en cas de prise de connaissance du dossier social).

### Menaces :

Accès illégitime au dossier du patient, impression ou photocopies de dossiers usagers, échange de mot de passe

### Sources de risques :

Source humaine interne malveillante, Source humaine interne accidentelle, Sinistre chez l'éditeur, source humaine externe agissant de manière délibérée

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

Chiffrement, Anonymisation, Gestion des postes de travail, Contrôle des accès logiques, Journalisation, Archivage, Contrôle d'intégrité, Sécurisation des documents papier, Sécurisation de l'exploitation, Sauvegarde des données

# Modification non désirée de données

### Impacts :

Défaut de prise en charge médico-sociale

### Menaces :

Usurpation d'identité, poste non verrouillé, erreur de manipulation

### Sources de risques :

Source humaine interne malveillante, Source humaine interne accidentelle, Source humaine extérieure malveillante

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

Chiffrement, Archivage, Contrôle des accès logiques, Sécurisation des documents papier

# Disparition de données

## Impacts :

Défaut de prise en charge du patient.

## Menaces :

Mauvaise manipulation, shutdown.

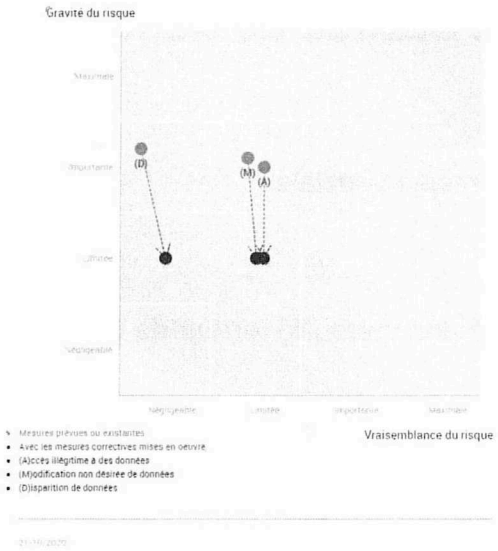
## Sources de risques :

Source humaine interne malveillante, Source humaine interne accidentelle, Source humaine extérieure malveillante, Source naturelle (incendie, inondation...)

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

Chiffrement, Contrôle des accès logiques, Archivage, Sauvegarde des données, Sécurisation de l'exploitation

# Cartographie des risques




| Nom et fonction<br>(Qualité de Directeur ou chef de Service requise) | Signature<br>(Précédée de la mention « **Lu et approuvé** ») |
|---|---|
| GERAADS Matthieu Directeur | Lu et approuvé<br>Matthieu GERAADS<br>Directeur de la Prévention et de l'Action Sociale |