



ORU Nouvelle Aquitaine

Version : 2.1

VEILLE SANITAIRE NOUVELLE AQUITAINE

Procédure d'alimentation automatique





Table des matières

1	Objectifs.....	3
2	Organisation.....	3
3	Principes	3
4	Procédure	4
4.1	Description Générale	4
4.2	Réalisation des tests unitaires	5
4.3	Description pas à pas	5
5	Définition des formats XML attendus	8
5.1	Formulaire SAMU	8
5.2	Formulaire RPU.....	8
6	Définition des formats de données attendus	10
6.1	Formulaire SAMU	10
6.2	Formulaire RPU.....	11
7	Sécurisation des échanges via GPG dans le cadre des transferts automatisés.....	14
7.1	Introduction.....	14
7.2	Préparation à l'utilisation de GPG – côté Acteurs	14
7.3	Chiffrement avec GPG – côté Acteur	15

Rédacteurs	Date de modification
Caroline Ligier, Abderrahmen Sahli	12/02/2025

1 Objectifs

Procédure de transmission automatisée des données de formulaires à destination du serveur de « veille sanitaire » du ROR Nouvelle Aquitaine.

2 Organisation

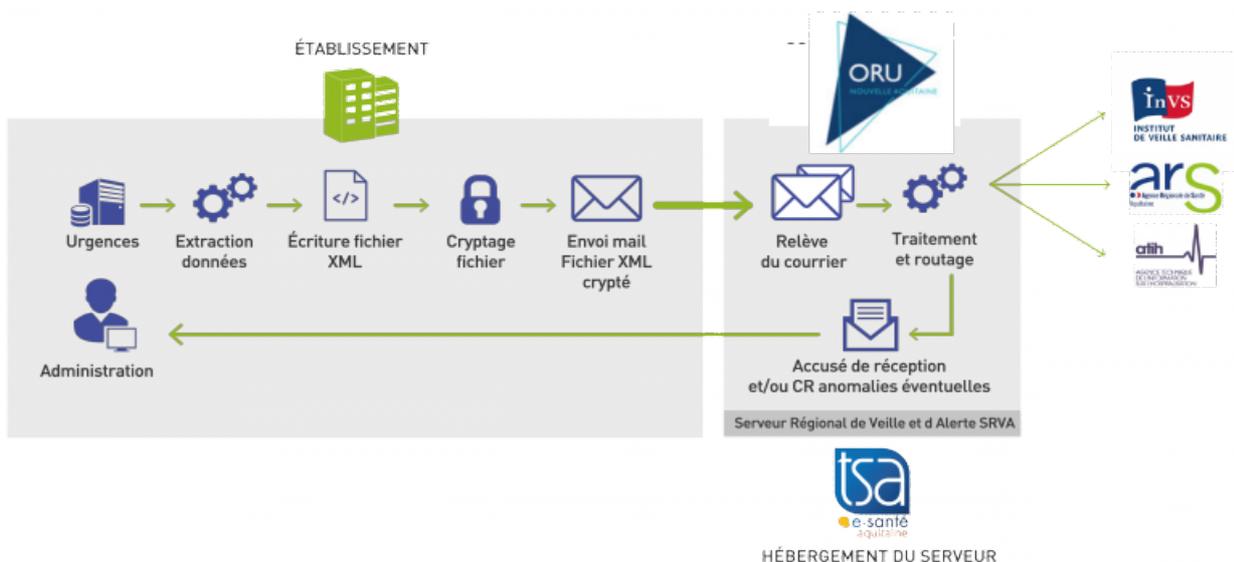
L'ARS Nouvelle Aquitaine collecte **quotidiennement** les données réglementaires de veille sanitaire sur un serveur dédié, alimenté par les établissements de soins. L'alimentation se fait par envoi d'un fichier crypté via ftp/sftp ou mail automatisé.

L'ORU NA joue le rôle d'intégrateur technique pour la réception des données envoyées par les établissements de santé et la transmission des indicateurs vers les structures telles que SpF ou l'ATIH.

Dans le cadre de la participation de l'établissement au dispositif OSCOUR (RPU), c'est le serveur régional de l'ARS qui alimentera automatiquement le serveur du réseau OSCOUR de SpF.

3 Principes

Transfert automatisé des données de Veille Sanitaire Nouvelle Aquitaine



4 Procédure

4.1 Description Générale

Chaque acteur doit mettre en place un module capable :

- d'extraire de son SIH, les données requises dans les formulaires qui lui sont attribués ;
- générer un fichiers ASCII normalisé au format XML selon les recommandations du GCS ORU Nouvelle Aquitaine.
- crypter individuellement les fichiers XML ;
- transmettre ces fichiers en pièces jointes d'un mail à l'adresse :
 - vs-ars@app.sante-aquitaine.net
- **ou** transmettre ces fichiers sur le serveur ftp/sftp régional

Pour obtenir un accès ftp/sftp il vous faut faire une demande d'identifiant à cie@oruna.fr avec les éléments suivants :

- Nom de l'établissement ;
- Plage d'adresses ip publiques qui enverront les fichiers ;
- Mail gpg afin d'échanger l'adresse IP du serveur FTP/SFTP et le couple login/mot de passe pour s'y connecter ou numéro de téléphone portable ou adresse de messagerie sécurisé ;

Le module proposé pour l'export doit pouvoir aisément évoluer sur les points suivants :

- Activation ou désactivation de la transmission ;
- Heure de transmission ;
- Clé publique pour la procédure de chiffrement ;
- Adresse email de l'automate d'import ;
- Identifiant fourni par l'ORU NA ;
- Clé d'authentification fournie par l'ORU NA ;

Chaque acteur souhaitant transmettre ses indicateurs par ce biais recevra, par les soins de l'ORU Nouvelle Aquitaine :

- une clé publique de cryptage ;
- un identifiant ;
- une clé d'authentification à intégrer dans chacune de ses transmissions ;



4.2 Réalisation des tests unitaires

Afin de vous aider dans la démarche d'envoi au serveur de veille sanitaire, vous pouvez prendre contact avec Mr Sahli de l'ORU Nouvelle Aquitaine au 06 18 37 23 29 ou abderrahmen.sahli@oruna.fr + cie@oruna.fr qui vous précisera les différentes étapes du protocole.

4.3 Description pas à pas

Étape 1

L'acteur depuis son propre SIH, extrait les données requises et constitue un fichier horodaté normalisé selon nos recommandations au format XML.

(Voir 5



Définition des formats XML attendus)

Le fichier généré à destination de l'ARS sera nommé de la manière suivante :

« **identifiant_AAAAMMDDHHMISS .xml** »

Exemple :

L'acteur ayant l'identifiant « 358 » qui extrait ses données du 02/07/07 le 03/07/07 à 08:15:00 nommera ses fichiers de la manière suivante :

- **358_20070703081500.xml** pour le fichier ARS

Étape 2

L'acteur crypte chacun des fichiers générés.

Les fichiers cryptés sont renommés **nom_du_fichier.gpg**.

Exemple :

- **358_20070703081500.xml.gpg** pour le fichier ARS

Étape 3

L'acteur transmet ces fichiers en pièces jointes d'un mail ou via FTP/SFTP

Adressé à : **vs-ars@app.sante-aquitaine.net**

Objet du message : **Extraction de données**

Étape 4

De son côté, le module d'intégration du serveur régional réalise les opérations suivantes :

- relève les messages transmis par les établissements ;
- décrypte les fichiers reçus ;
- vérifie l'identité et authentifie l'expéditeur ;
- vérifie l'intégrité des données reçues ;
- redistribue les indicateurs aux différents acteurs (ARS, DHOS, SpF, ATIH) en fonction de leurs besoins ;
- envoie, si requis, un message de compte rendu de bonne exécution du traitement.

Les données de **Résumé de Passage aux Urgences (RPU)** doivent impérativement être transmises **quotidiennement avant 06h00 du matin** et contenir l'intégralité des passages des **7 derniers jours**. Les Résumés de Passage aux Urgences correspondent à l'ensemble des passages ayant une date et heure d'entrée renseignées.



Dans le cadre des campagnes de **validation des données RPU** qui ont lieu deux fois dans l'année (en janvier et en septembre), les RPU doivent impérativement pouvoir être **rejouées via le même canal** de transmission que l'envoi quotidien avec une possibilité de reprise de **l'année précédente**.

Les données agrégées **SAMU** doivent impérativement être transmises **avant 09h00**, et contenir les données des **4 derniers jours**. Les données agrégées Urgence correspondent à l'ensemble des passages sur 24 heures, que le patient soit sorti ou non du service d'urgence et sont alimenté automatiquement via le RPU.

Un même fichier peut contenir plusieurs types de formulaires, tant qu'ils sont contenus dans des balises <element /> (cf. définition des formats XML attendus).

En cas d'anomalie, un message est retourné à l'expéditeur signalant le dysfonctionnement.

5 Définition des formats XML attendus

5.1 Formulaire SAMU

```

<result>
  <entete>
    <idActeur>Identifiant de l'acteur en cours</idActeur>
    <cleActeur>Clé unique attribuée à l'acteur</cleActeur>
    <arRequis>Indicateur d'envoi d'accusé reception</arRequis>
    <mail>Adresse email d'envoi d'accusé reception de bon ou mauvais fonctionnement</mail>
  </entete>
  <element>
    <nomForm>SAMU</nomForm>
    <date_event>Date de l'événement en cours</date_event>
    <NbD>Valeur en cours</NbD>
    <NbAffaires>Valeur en cours</NbAffaires >
    <NbDRMglobal>Valeur en cours</NbDRMglobal>
    <NbDRMglobal0>Valeur en cours</NbDRMglobal0>
    <NbDRMglobal8>Valeur en cours</NbDRMglobal8>
    <NbDRMglobal12>Valeur en cours</NbDRMglobal12>
    <NbDRMglobal20>Valeur en cours</NbDRMglobal20>
    <NbDRMAMU>Valeur en cours</NbDRMAMU>
    <NbDrmCovid19>Valeur en cours</NbDrmCovid19>
    <NbDRMLIB>Valeur en cours</NbDRMLIB>
    <ActivationCellCrise>Valeur en cours</ActivationCellCrise>
    <DelestAppel>Valeur en cours</DelestAppel>
    <RenfortPers>Valeur en cours</RenfortPers>
  </element>
</result>

```

5.2 Formulaire RPU

Le format OSCOUR est aussi accepté.

```

<result>
  <entete>
    <idActeur>Identifiant de l'acteur en cours</idActeur>
    <cleActeur>Clé unique attribuée à l'acteur</cleActeur>
    <arRequis>Indicateur d'envoi d'accusé reception</arRequis>
    <mail>Adresse email d'envoi d'accusé reception de bon ou mauvais fonctionnement</mail>
  </entete>
  <element>
    <nomForm>RPU</nomForm>
    <date_event>Date d'entrée du patient</date_event>
    <CP>Valeur en cours</ CP >
    <COMMUNE>Valeur en cours</COMMUNE>
    <NAISSANCE>Valeur en cours</NAISSANCE>
    <SEXE>Valeur en cours</SEXE>
    <ENTREE>Valeur en cours</ENTREE>
  </element>
</result>

```



Flux Veille Sanitaire ROR Nouvelle Aquitaine

```
<MODE_ENTREE>Valeur en cours </MODE_ENTREE>
<PROVENANCE>Valeur en cours </PROVENANCE>
<TRANSPORT>Valeur en cours </TRANSPORT>
<TRANSPORT_PEC>Valeur en cours </TRANSPORT_PEC>
<MOTIF>Valeur en cours </ MOTIF >
<GRAVITE>Valeur en cours </ GRAVITE >
<DP>Valeur en cours </ DP >
<LISTE_DA>
    <DA>Valeur en cours </DA>
    <DA>Valeur en cours </DA>
....
</LISTE_DA>
<LISTE_ACTES>
    <ACTE>Valeur en cours </ ACTE >
    <ACTE>Valeur en cours </ ACTE >
....
</LISTE_ACTES>
<SORTIE>Valeur en cours</ SORTIE >
<MODE_SORTIE>Valeur en cours</ MODE_SORTIE >
<DESTINATION>Valeur en cours</ DESTINATION >
<ORIENT>Valeur en cours</ ORIENT >
</element>
.....
</result>
```

6 Définition des formats de données attendus

6.1 Formulaire SAMU

<i>Balise</i>	<i>Description</i>	<i>Type</i>	<i>Format et observations</i>
<idActeur>	Identifiant de l'acteur en cours	Entier	Fourni par l'ORU NA
<cleActeur>	Clé unique attribuée à l'acteur	Caractères	Fourni par l'ORU NA
<arRequis>	Indicateur d'envoi d'accusé réception	Entier	1 = Accusé Réception. 0 = Pas d'accusé requis.
<mail>	Adresse email d'envoi d'accusé réception de bon ou mauvais fonctionnement	Caractères	xxx@xxx.xx
<nomForm>	Code du formulaire	Caractères	SAMU
<date_event>	Date de l'événement en cours	Caractères	jj/mm/aaaa
<NbD>	Nombre de D global hors DR et DRM /24h <i>Précisions : appels malveillants ou erreur de numéro</i>	Entier	Supérieur ou égal à 0
<NbAffaires>	Nombre de DR global hors DRM /24h <i>Précisions : appel administratif, demande de renseignement, transmission information opérationnel, prise en charge sociale, ouverture de poste de secours..</i>	Entier	Supérieur ou égal à 0
<NbDRMglobal>	Nombre de DRM global /24h	Entier	Supérieur ou égal à 0
<NbDRMglobal8>	Nombre de DRM entre 08h-12h	Entier	Supérieur ou égal à 0
<NbDRMglobal12>	Nombre de DRM entre 12h-20h	Entier	Supérieur ou égal à 0
<NbDRMglobal20>	Nombre de DRM entre 20h-00h	Entier	Supérieur ou égal à 0
<NbDRMglobal0>	Nombre de DRM entre 00h-08h	Entier	Supérieur ou égal à 0
<NbDrmCovid19>	Nombre de DRM COVID-19 /24h	Entier	Supérieur ou égal à 0
<NbDRMLIB>	Nombre de Dossiers de Régulation Médicale assurés par les médecins libéraux de la Permanence de soins	Entier	Supérieur ou égal à 0
<NbDRMAMU>	Nombre de Dossiers de Régulation Médicale assurés par l'Aide Médicale d'Urgences	Entier	Supérieur ou égal à 0
<ActivationCellCrise>	ACTIONS DE GESTION C-15 Activation de la cellule de crise du SAMU	Caractères	Oui Non
<DelestAppel>	ACTIONS DE GESTION C-15 Delestage des appels vers un autre centre de regulation	Caractères	Oui Non
<RenfortPers>	ACTIONS DE GESTION C-15 Renfort du personnel (PARM, medecins regulateurs)	Caractères	Oui Non

Flux Veille Sanitaire ROR Nouvelle Aquitaine

6.2 Formulaire RPU

<i>Balise</i>	<i>Description</i>	<i>Type</i>	<i>Format et observations</i>
<idActeur>	Identifiant de l'acteur en cours	Entier	Fourni par l'ORU NA
<cleActeur>	Clé unique attribuée à l'acteur	Caractères	Fourni par l'ORU NA
<arRequis>	Indicateur d'envoi d'accusé réception	Entier	1 = Accusé Réception. 0 = Pas d'accusé requis.
<mail>	Adresse email d'envoi d'accusé réception de bon ou mauvais fonctionnement	Caractères	xxx@xxx.xx
<nomForm>	Code du formulaire	Caractères	RPU
<date_event>	Date d'entrée du patient	Caractères	JJ/MM/AAAA
<CP>	Code postal de résidence: - Si le code postal précis est inconnu: n° de département suivi de 999 - Pour les patients résidant hors de France: 99 suivi du code INSEE du pays - Si département ou pays de résidence inconnu: 99999	Caractères	
<Commune>	Nom de la commune de résidence	Caractères	
<NAISSANCE>	Date de naissance (vide correspond à date de naissance incertaine, demande d'anonymat par le patient, droit CNIL exprimé par le patient pour suppression des informations le concernant))	Caractères	JJ/MM/AAAA
<SEXE>	Sexe (I pour indéterminé)	Caractères	M / F / I
<ENTREE>	Date et heure de la prise en charge administrative du patient	Caractères	JJ/MM/AAAA HH:MM
<MODE_ENTREE>	Mode d'entrée PMSI 6 : mutation / 7 : transfert / 8 : domicile	Entier	6 / 7 / 8
<PROVENANCE>	Provenance PMSI Entrée par mutation ou transfert: 1: provenance unité de soins MCO 2: provenance unité de soins de suite ou réadaptation 3: provenance unité de soins longue durée 4: provenance unité de psychiatrie Entrée à partir du domicile: 5: prise en charge aux urgences autres que pour des raisons organisationnelles 6 : hospitalisation à domicile 7 : structure d'hébergement médicosociale 8: prise en charge aux urgences pour des raisons organisationnelles	Entier	1 / 2 / 3 / 4 / 5 / 6 / 7 / 8

Flux Veille Sanitaire ROR Nouvelle Aquitaine

<i>Balise</i>	<i>Description</i>	<i>Type</i>	<i>Format et observations</i>
	(patients reconvoqués pour des soins à distance, admission pour faciliter enregistrement administratif, ou réalisation d'exams complémentaires...)		
<TRANSPORT>	Mode de transport lors de l'entrée du patient dans le service PERSO : personnel AMBU : ambulance privée ou publique VSAB : véhicules de secours et d'aide aux victimes SMUR : véhicule du Service Mobile d'Urgence et Réanimation HELI : hélicoptère FO : Force de l'Ordre	Caractères	PERSO / AMBU / VSAB / SMUR / HELI / FO
<TRANSPORT_PEC>	Mode de prise en charge durant le transport MED : médicalisé PARAMED : paramédicalisé AUCUN : absence de médicalisation ou par-médicalisation	Caractères	MED / PARAMED / AUCUN
<MOTIF>	Motif du recours aux urgences : thésaurus SFMU	Caractères	THESAURUS SFMU
<GRAVITE>	Classification CCMU enrichie	Entier	1 / 2 / 3 / 4 / 5 / P / D
<DP>	Diagnostic principal	Caractères	Code CIM10
<LISTE_DA> <DA></DA>	Diagnostic associé	Caractères	Code CIM10
<LISTE_ACTES> <ACTE></ACTE>	Actes réalisés aux urgences: Saisir les 7 premiers caractères au minimum	Caractères	Code CCAM
<SORTIE>	Date et heure de sortie	Caractères	JJ/MM/AAAA HH:MM
<MODE_SORTIE>	Mode de sortie PMSI 6= mutation 7= transfert 8= domicile 9= Décés	Entier	6 / 7 / 8 / 9
<DESTINATION>	Destination PMSI Sortie par mutation ou transfert: 1= Hospitalisation dans une unité MCO 2= Hospitalisation dans une unité de soins de suite ou réadaptation 3= Hospitalisation dans une unité de soins de longue durée 4= Hospitalisation dans une unité psychiatrique Sortie au domicile 6= Retour au domicile dans le cadre d'une hospitalisation à domicile 7= Retour vers une structure d'hébergement médico-social	Entier	1 / 2 / 3 / 4 / 6 / 7
<ORIENT>	Orientation précision du devenir ou des circonstances associées - Sortie par mutation ou transfert HDT = Hospitalisation à la demande d'un tiers HO = Hospitalisation d'office SC = Hospitalisation en surveillance continue SI = Hospitalisation en Soins Intensifs REA = Hospitalisation en unité de réanimation UHCD : Hospitalisation dans une unité d'hospitalisation de courte	Caractères	FUGUE / SCAM / PSA / REO / SC / SI / REA / UHCD / MED / CHIR / OBST / HDT / HO

Flux Veille Sanitaire ROR Nouvelle Aquitaine

<i>Balise</i>	<i>Description</i>	<i>Type</i>	<i>Format et observations</i>
	<p>durée</p> <p>MED= Hospitalisation dans une Unité de Médecine hors SC, SI ou REA</p> <p>CHIR= Hospitalisation dans une Unité de chirurgie hors SC, SI ou REA</p> <p>OBST: Hospitalisation dans une Unité d'obstétrique hors SC, SI ou REA</p> <p>- Sortie au domicile</p> <p>FUGUE: sortie à l'insu du personnel soignant</p> <p>SCAM: sortie contre avis médical</p> <p>PSA: parti sans attendre la prise en charge</p> <p>REO: réorientation directe (consultation spécialisée ou service d'accueil administratif fermé)</p>		

Pensez à encapsuler les champs texte avec des balises `<![CDATA[]]>` afin d'éviter les problèmes de corruption des fichiers xml avec des accents ou autres caractères spéciaux.

7 Sécurisation des échanges via GPG dans le cadre des transferts automatisés

7.1 Introduction

Les fichiers amenés à être transmis par messagerie électronique seront préalablement chiffrés.

L'outil utilisé pour le chiffrement des fichiers est le logiciel GnuPG dans sa dernière version stable.

Ce logiciel est la version gratuite et libre du standard de cryptographie forte OpenPGP.

Les guides d'utilisation, FAQ, sources et binaires du logiciel sont disponibles sur le site <http://www.gnupg.org> et sur de nombreux miroirs référencés depuis cette même adresse.

Une paire de clé privée/publique sera générée par la veille ARS. La veille ARS détiendra la clé privée et fournira sa clé publique aux entités ayant à lui transmettre des fichiers.

7.2 Préparation à l'utilisation de GPG – côté Acteurs

Du côté « émetteur des fichiers – utilisateur de la clé publique » deux opérations sont nécessaires :

- importation de la clé publique
- trust de cette clé

Importation de la clé publique

On doit importer la clé publique fournie par la veille ARS dans le trousseau de clés de GPG

Pour cela on va indiquer à GPG de récupérer la clé depuis le fichier texte qui aura été fourni.

```
gpg --import "pubkey-veille-arh.txt"
```

Une fois la clé importée avec succès, on pourra afficher son fingerprint pour vérifier que l'on a bien importé la bonne clé .

```
gpg --fingerprint vs-arh@sante-aquitaine.org
```



Trust de la clé

A l'utilisation de GPG pour chiffrer avec une clé publique non trustée le message suivant s'affiche :

*« It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.
Use this key anyway ?) »*

On doit donc déclarer la clé importée comme « de confiance » afin d'éviter les messages d'avertissement à chaque utilisation de cette clé :

```
gpg --edit-key vs-arh@sante-aquitaine.org  
Command> trust
```

Choisir de faire confiance complètement à cette clé : Yes

7.3 Chiffrement avec GPG – côté Acteur

Chiffrement d'un fichier avec la clé publique veille ARH

Exemple : Nous allons chiffrer le fichier fichier-test.pdf :

```
gpg -r vs-arh@sante-aquitaine.org --encrypt fichier-test.pdf
```

Nous récupérons le fichier chiffré avec une double extension fichier-test.pdf.gpg