VACCIN-COVID

AIPD

Table des matières

Vue d'ensemble

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

Le système d'information « Vaccin Covid », créé par le décret 2020-1690 du 25 décembre 2020, est l'objet de la présente analyse d'impact sur la protection des données. Toutefois et compte tenu du peu de temps qui a été alloué aux responsables de traitement, certaines briques logicielles associées à des finalités ou sous-finalités n'ont pas encore été mises en œuvre comme nous l'indiquons plus bas dans ce document.

C'est le cas notamment des transferts des données à la direction du numérique du ministère pour le compte de la DGS, des ARS et de la DREES qui n'ont pas encore fait et qui nécessiteront la mise à jour de ce document dès lors que les flux seront effectifs.

Dans le contexte de la pandémie de Covid-19 et avec l'arrivée fin 2020 des premiers vaccins sur le marché, il est nécessaire d'organiser une vaccination rapide et prudente de la population.

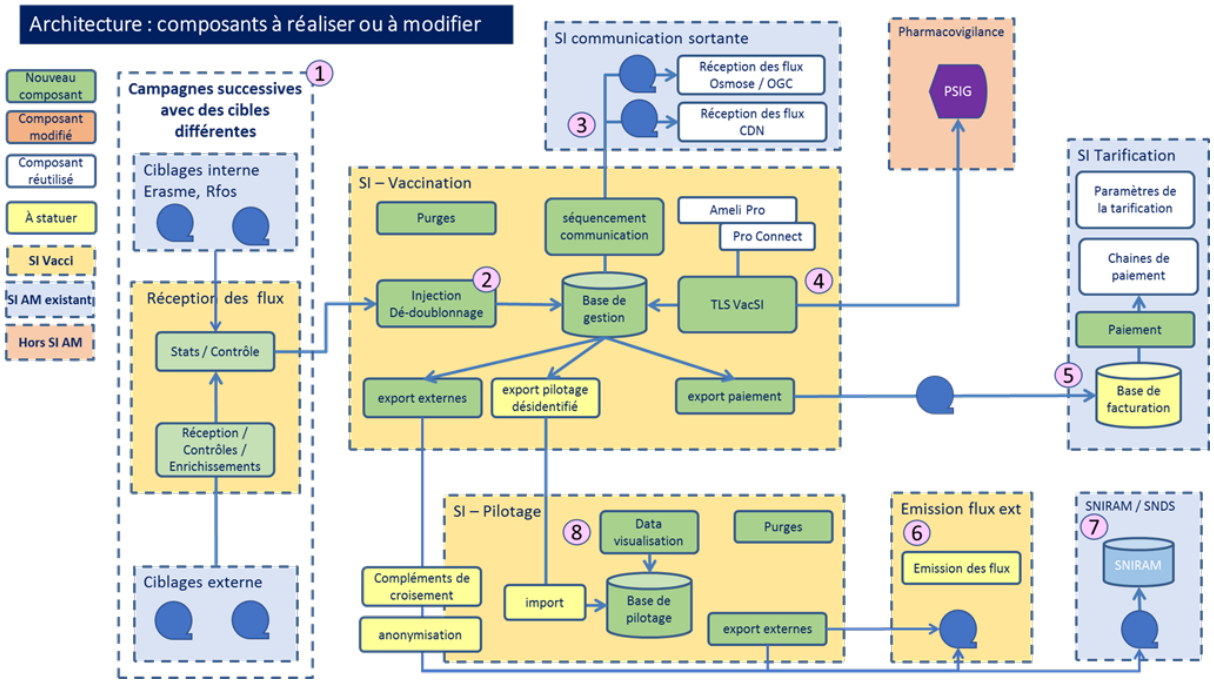
Conformément au décret n°2020-1690 du 25 décembre 2020, est autorisée la création d'un traitement automatisé de données à caractère personnel dans le cadre de la campagne de vaccination contre la covid-19, dénommé " Vaccin Covid ".

La création du système d'information « Vaccin Covid » a pour objectif de permettre la mise en œuvre d'une campagne de vaccination contre le Sars-Cov-2.

Ce traitement a pour finalités :

- L'identification des personnes éligibles à la vaccination au regard des recommandations énoncées par le ministre chargé de la santé en application des dispositions de l'article L. 3111-1 du code de la santé publique, l'envoi de bons de vaccination à ces personnes, l'accompagnement à la vaccination des personnes présentant des vulnérabilités de santé particulières, l'enregistrement des informations relatives à la consultation préalable à la vaccination et l'organisation de la vaccination de ces personnes ;
- Le suivi de l'approvisionnement des lieux de vaccinations en vaccins et consommables ;
- L'envoi à la personne vaccinée d'un récapitulatif des informations relatives à la vaccination, établi par le professionnel de santé réalisant la vaccination ou par le personnel placé sous sa responsabilité ;
- La mise à disposition de données permettant la présentation de l'offre de vaccination, la surveillance de la couverture vaccinale, la mesure de l'efficacité et de la sécurité vaccinales, la pharmacovigilance, le suivi statistique de la campagne de vaccination, l'appui à l'évaluation de la politique publique de vaccination et la réalisation d'études et de recherches, et l'adaptation des mesures médicales d'isolement prophylactiques pour les personnes vaccinées identifiées comme cas contact ou personnes co-exposées en application des dispositions de l'article 1er du décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions ;
- La délivrance, en cas d'apparition d'un risque nouveau, de l'information prévue à l'article L. 1111-2 du code de la santé publique, aux personnes vaccinées et, le cas échéant, leur orientation vers un parcours de soins adaptés ;
- La prise en charge financière des actes liés à la vaccination ;
- La mise à disposition de données permettant le contrôle de l'obligation vaccinale des personnes mentionnées au deuxième alinéa du II de l'article 13 de la loi n° 2021-1040 du 5 août 2021 relative à la gestion de la crise sanitaire.

L'ensemble des finalités reposant, à date, sur l'infrastructure fonctionnelle simplifiée ci-dessous



Dans le cadre de ce traitement, les personnes concernées sont :

- Toute personne possiblement éligible à la vaccination sur la base de la stratégie vaccinale définie par le gouvernement à partir des recommandations de la HAS
- Les professionnels de santé, et personnes placées sous leur responsabilité, participant au cycle de vaccination
- Possiblement les médecins traitants au sens du code de la sécurité sociale
- De manière plus résiduelle, certains agents administrateurs (données de traçabilité au SI)

Quelles sont les responsabilités liées au traitement ?

Le traitement des données à caractère personnel présentes dans le système d'information « VaccinCovid» est placé sous **la responsabilité conjointe** de la direction générale de la santé (DGS) et de la caisse nationale de l'assurance maladie (Cnam). Un accord de coresponsabilité détermine les rôles et obligations de chaque responsable conjoint.

	Ministère/DGS	**CNAM**
Pilotage / Pouvoir de décision de mise en œuvre :		
Si le traitement répond à une mission publique, quel est l'organisme chargé de remplir cette mission ?	X	X
Qui détermine les finalités du traitement (qui a décidé de la mise en œuvre du traitement, du « pourquoi » le traitement est mis en place, de ses objectifs, du résultat attendu, des éléments de cadrage) ?	X	
Qui est chargé de la mise en œuvre du traitement ?	X	X
Qui prend la responsabilité d'homologuer le traitement/SI ? Qui est l'autorité d'homologation ?	X	
Instructions préalables données (degré d'autonomie) :		
Qui donne les instructions concernant le traitement lors de la phase de construction du projet (SI/traitement) ? (détermination du « comment » arriver au résultat : donneur(s) d'ordres, directives pour construire le traitement, arbitrage)	Comité stratégique, avec, en cas de différent, recours à un arbitrage du ministre de la santé ou de son cabinet	
Qui fournit les moyens humains et financiers lors de la phase de construction du projet (SI/traitement) ?	X	X
Qui réalise et met à jour l'analyse d'impacts sur la protection des données (AIPD) ?	X	X
Qui assure la tenue du registre du traitement ?	X	X
Lorsque des formalités auprès de la CNIL sont nécessaires (avis sur un texte, demande d'autorisation, soumission de l'AIPD, mesures de transparence…) : quel(s) RT(s) effectue(nt) les démarches pour le traitement ?	X	X
Qui définit les données à caractère personnel à collecter/traiter dans le cadre du traitement pour atteindre la finalité (qui veille à la minimisation des données/quantité, profondeur des données) ?	X	
Qui détermine quels sont les destinataires des données traitées ?	X	
Autonomie du/des RT une fois le traitement déployé		
Qui donne les instructions une fois le traitement déployé et utilisé par le(s) métier(s) ?	X	
Qui fournit les moyens humains une fois le traitement déployé/utilisé par le(s) métier(s) ?		X
Qui notifie l'information à la CNIL en cas de violation de données ?	Pour les notifications	Notification portée par la

	mentionnées au 5. 1.c en coordination avec la DPD du ministère, le service du HFDS et la CNAM	CNAM, mais à coordonner avec le ministère
Qui notifie l'information aux personnes concernées (usagers-patients et utilisateurs-professionnels sanitaire et médico-social), si nécessaire, en cas de violation de données ? (Une circulation de l'information doit être prévue dans l'accord en amont entre les RT, quel que soit le RT qui informe les personnes concernées.)	X	X
Qui détermine les personnes habilitées à appeler le téléservice ? (politique de confidentialité/gestion des habilitations)	X	
Surveillance (maîtrise des opérations)		
Qui vérifie l'avancée du projet et demande des comptes régulièrement auprès des acteurs ?	X (Comité de suivi)	X (comité de suivi)
Qui vérifie que les instructions données sont correctement exécutées et le bon fonctionnement du traitement	X (Comité de suivi)	X (Comité de suivi)
Visibilité		
Qui est présenté aux personnes concernées (utilisateurs et patients) comme leur interlocuteur/le RT pour le traitement ?	X	X
Qui informe les personnes concernées conformément au RGPD (protection des données) ?	X	X
Qui met en place les modalités d'exercice des droits des personnes concernées (accès, rectification, opposition…) ?		X
Qui se chargera de répondre aux demandes relatives à l'exercice des droits des personnes ? (modalités de transmission entre les responsables conjoints à prévoir dans l'accord)		X Directement auprès de la caisse de rattachement
Expertise technique/sécurité		
Quelle entité définit, au regard des propositions et expertises, le niveau de risque résiduel acceptable eu égard aux nécessités d'usage ?	X	X
Quelle entité vérifie l'adéquation du traitement à la doctrine technique du numérique en santé ?	X	x
Quelle est l'entité qui met en œuvre l'analyse des évolutions techniques à apporter pour l'amélioration de l'infrastructure technique, de la sécurité ? (Disponibilité, performance, chiffrement, pseudonymisation éventuelle, traçabilité, revue des accès, etc.)	X	X

Quelle est l'entité qui décide des évolutions mineures à apporter concernant ces domaines ?	X	X
Quelle est l'entité qui décide des évolutions majeures à apporter concernant ces domaines ?	X	X
Quelle est l'entité qui met en œuvre les évolutions concernant ces domaines ?	x	X

Les RT peuvent être amenées à sous-traiter la mise en œuvre de certaines fonctionnalités couvertes par le système d'information.

Le ciblage des personnes éligibles à la vaccination reposera, en partie, sur les traitements de données déjà mis en œuvre par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie au titre de leurs missions (ex : données de remboursement). Les responsables de traitement pourront donc demander aux organismes des autres régimes de :

- procéder aux opérations de ciblage dans leurs bases de données conformément aux critères qu'ils auront fixés,
- transmettre les données d'identification des personnes ciblées à la Cnam pour intégration dans la base « Vaccin Covid».

Ces organismes seront alors qualifiés de sous-traitants au sens de la loi « informatique et libertés » dans la mesure où ils procéderont aux opérations de traitement « au nom et pour le compte » des responsables de traitements (détermination des finalités, des critères et des moyens par les responsables de traitement). Des clauses RGPD sont inscrites dans les contrats signés avec chaque sous-traitant.

Par ailleurs, les responsables de traitement traitent également avec :

- **Wordline** qui est titulaire d'un marché global avec l'assurance maladie pour les campagnes sortantes (pas un marché dédié vaccin covid),
- **La Direction du Numérique (DNUM)** du ministère des solidarités et de la santé sera chargée par la DGS de l'élaboration des tableaux de bord regroupant des indicateurs de pilotage mais également la mise sous séquestre des données de vaccination. L'envoi des données par la CNAM à la DNUM s'effectuant par un mécanisme automatisé n'impliquant aucune intervention humaine. Pour ces deux missions, une convention a été signée entre la DGS et la DNUM.

Quels sont les référentiels applicables ?

Référentiels sécurité

RGS
PSSI-MCAS

Référentiels juridiques

RGPD
Décret n° 2020-1690 du 25 décembre 2020 autorisant la création d'un traitement de données à caractère personnel relatif à la gestion et au suivi des vaccinations contre le coronavirus SARS COV2

Données, processus et supports

Quelles sont les données traitées ?

Les données à caractère personnel et les informations enregistrées dans le présent traitement sont les suivantes :

1° Les données d'identification de la personne éligible à la vaccination, vaccinée ou non vaccinée : nom, prénoms, sexe, date de naissance, lieu de naissance, numéro d'inscription au répertoire national d'identification des personnes physiques ou, le cas échéant, code d'admission au bénéfice de l'aide médicale d'Etat sous la mention immatriculation ;

2° Le code du régime d'affiliation et de l'organisme gestionnaire assurant la prise en charge des frais de santé de la personne mentionnée au 1°du décret n° 2020-1690;

3° Les coordonnées de la personne mentionnée au 1° du décret n° 2020-1690 et de son représentant légal éventuel : adresse postale, numéro de téléphone, adresse électronique ;

4° Les références du ou des bons de vaccination délivrés à la personne ;

5° Les données relatives à la réalisation de la vaccination : dates de la, ou des injections, informations permettant l'identification du vaccin injecté, précisions sur l'administration du vaccin, identification du ou des lieux de vaccination, identification des professionnels de santé ayant réalisé respectivement la consultation préalable à la vaccination et chaque injection ;

6° Les données relatives à la santé de la personne mentionnée au 1° du décret n° 2020-1690:

a) Critères médicaux d'éligibilité à la vaccination et traitements suivis ;

b) Informations relatives à la recherche et à l'identification de contre-indications à la vaccination ;

c) Effets indésirables éventuels associés à la vaccination ;

d) Date d'une infection par le virus de la covid-19 obtenue à partir des informations mentionnées au 6° de l'article 9 du décret du 12 mai 2020 susmentionné ;

7° Les informations sur les critères d'éligibilité non médicaux à la vaccination ;

8° Les données d'identification des professionnels de santé, et des personnes placées sous leur responsabilité, ayant réalisé la consultation préalable et la vaccination : données d'identification, coordonnées et numéro d'identification de l'établissement ou de la structure de rattachement, de l'établissement ou de la structure de vaccination.
Les données mentionnées au titre du présent article ne peuvent révéler directement ou indirectement la qualité de militaire, à l'exclusion de celles mentionnées aux 2° et 8°.

En annexe 2, un tableau détaille les catégories de données, le détail des données, les sources des données ainsi que les destinataires selon le type de données

En annexe 3, un tableau précise les différents niveaux de pseudonymisation selon les destinataires des données

Sont destinataires des données enregistrées dans le traitement :

1° Les professionnels de santé réalisant la consultation préalable et la vaccination, ainsi que les personnes placées sous leur responsabilité, pour l'ensemble des données mentionnées à l'article 2 du décret du 25 décembre 2020, à l'exclusion de celles visées au a) du 6° , à savoir les critères médicaux d'éligibilité à la vaccination et traitements suivis

;

2° Le médecin traitant de la personne vaccinée, au sens de l'article L. 162-5-3 du code de la sécurité sociale, pour les données mentionnées au 1°, 5°, 6° et 8° de l'article 2 du décret. Il s'agit des données suivantes :

Les données d'identification de la personne invitée à se faire vacciner ou vaccinée : nom, prénoms, sexe, date de naissance, lieu de naissance, numéro d'inscription au répertoire national d'identification des personnes physiques ou, le cas échéant, code d'admission au bénéfice de l'aide médicale d'Etat sous la mention immatriculation

Les données relatives à la réalisation de la vaccination : dates de la, ou des injections, informations permettant l'identification du vaccin injecté, précisions sur l'administration du vaccin, identification du ou des lieux de vaccination, identification des professionnels de santé ayant réalisé respectivement la consultation préalable à la vaccination et chaque injection

Les données d'identification des professionnels de santé, et des personnes placées sous leur responsabilité, ayant réalisé la consultation préalable et la vaccination : données d'identification, coordonnées et numéro d'identification de l'établissement ou de la structure de rattachement, de l'établissement ou de la structure de vaccination. ;

3° Pour leurs ressortissants, les agents des organismes des régimes obligatoires d'assurance maladie, individuellement habilités par le directeur de chaque organisme, pour les données mentionnées à l'article 2, à l'exclusion des données mentionnées au 6° (cf 1° dessus) ;

4° La direction du numérique des ministères chargés des affaires sociales, en tant que tiers de confiance désigné par le directeur général de la santé, aux seules fins de permettre l'orientation des personnes vers un parcours de soin adapté en cas de risque nouveau, pour les seules données mentionnées au 1° et 5° de l'article 2 du décret :

Les données d'identification de la personne vaccinée : nom, prénoms, sexe, date de naissance, lieu de naissance, numéro d'inscription au répertoire national d'identification des personnes physiques ou, le cas échéant, code d'admission au bénéfice de l'aide médicale d'Etat sous la mention immatriculation

Les données relatives à la réalisation de la vaccination : dates de la ou des injections, informations permettant l'identification du vaccin injecté, précisions sur l'administration du vaccin, identification du ou des lieux de vaccination, identification des professionnels de santé ayant réalisé respectivement la consultation préalable à la vaccination et chaque injection ;

5° La caisse nationale d'assurance maladie, pour les données mentionnées au 1°, 4°, 5°, 6°, et 7° de l'article 2 du décret, en vue de leur versement dans le dossier médical partagé de la personne vaccinée. Ces données sont donc

Les données d'identification de la personne invitée à se faire vacciner ou vaccinée : nom, prénoms, sexe, date de naissance, lieu de naissance, numéro d'inscription au répertoire national d'identification des personnes physiques ou, le cas échéant, code d'admission au bénéfice de l'aide médicale d'Etat sous la mention immatriculation

Les références du ou des bons de vaccination délivrés à la personne

Les données relatives à la réalisation de la vaccination : dates de la ou des injections, informations permettant l'identification du vaccin injecté, précisions sur l'administration du vaccin, identification du ou des lieux de vaccination, identification des professionnels de santé ayant réalisé respectivement la consultation préalable à la vaccination et chaque injection

Les informations sur les critères d'éligibilité non médicaux à la vaccination ;

6° L'Agence nationale de sécurité du médicament et des produits de santé et les centres régionaux de pharmacovigilance, pour l'exercice de leur mission de pharmacovigilance, pour les seules données mentionnées au 1° limitées aux trois premières lettres du nom et du prénom, la date de naissance et le sexe, ainsi que les données mentionnées au 5°, 6° et 7° de l'article 2 du décret ;

Les données relatives à la réalisation de la vaccination : dates de la ou des injections, informations permettant l'identification du vaccin injecté, précisions sur l'administration du vaccin, identification du ou des lieux de vaccination, identification des professionnels de santé ayant réalisé respectivement la consultation préalable à la vaccination et chaque injection ;

Les informations sur les critères d'éligibilité non médicaux à la vaccination

7° Le service public d'information en santé prévu par l'article L.1111-1-1 du code de la santé publique, pour les seules données mentionnées au 5° et 8° de l'article 2 du décret nécessaires à sa mission de diffusion gratuite auprès du public de l'offre de soins disponible. . Ces données sont :

Les données relatives à la réalisation de la vaccination : dates de la ou des injections, informations permettant l'identification du vaccin injecté, précisions sur l'administration du vaccin, identification du ou des lieux de vaccination, identification des professionnels de santé ayant réalisé respectivement la consultation préalable à la vaccination et chaque injection

Les données d'identification des professionnels de santé, et des personnes placées sous leur responsabilité, ayant réalisé la consultation préalable et la vaccination : données d'identification, coordonnées et numéro d'identification de l'établissement ou de la structure de rattachement, de l'établissement ou de la structure de vaccination

Sont destinataires de données ayant fait l'objet de mesures adéquates de pseudonymisation permettant d'assurer la confidentialité de l'identité des personnes :

1° Les personnes habilitées par le directeur général de l'Agence nationale de santé publique, pour les données nécessaires au suivi de la couverture vaccinale et à la mesure de l'efficacité vaccinale ;

2° Les personnes habilitées par les directeurs généraux des agences régionales de santé, pour les données nécessaires à l'organisation de la campagne de vaccination à l'échelon régional et à son suivi ;

3° Les personnes habilitées par le directeur de la recherche, des études, de l'évaluation et des statistiques du ministère chargé de la santé, pour les données nécessaires à sa mission d'analyse et de diffusion des informations statistiques dans le domaine de la santé ;

4° Le groupement d'intérêt public mentionné à l'article L. 1462-1 du code de la santé publique et la Caisse nationale de l'assurance maladie aux seules fins de faciliter l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le virus.

Les personnes accédant au SI

Les agents de l'Assurance Maladie n'ont pas vocation à accéder au SI vaccination dans sa version « données directement identifiantes ».

Certains agents de l'Assurance Maladie pourront disposer d'un accès à l'application, après habilitation, afin de permettre la délivrance des attestations certifiées de vaccination, aux personnes ne disposant pas des équipements informatiques pour le faire.

Les administrateurs de base en nombre restreints pourront accéder à la base notamment pour pouvoir faire les corrections et gestions d'anomalies ainsi que pour opérer la purge des données suite à un droit d'opposition. Ces accès sont réalisés sur la base chiffrée et, pour pouvoir résoudre un cas individuel, ils doivent alors obtenir une autorisation ad hoc pour le déchiffrement.

Des accès par des agents AM pourront être envisagés dans une version ultérieure pour intégrer de nouvelles fonctionnalités (alimentation DMP, envoi aux MT) ;

Par ailleurs, un profil particulier est créé pour accéder à la fonction pilotage pour les agents AM avec un accès à des données de-identifiées (base SI Pilotage).

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

1. Le ciblage et l'envoi des invitations

a. Le ciblage par l'assurance maladie

L'identification des personnes concernées par les phases de la vaccination s'effectue depuis les bases de données de l'assurance maladie via des requêtes. Ces requêtes utilisent des critères élaborés en déclinaison des recommandations de la HAS qui, en retour, peuvent conduire à utiliser telle ou telle autre source de données disponibles.

L'élaboration des critères et des requêtes étant actuellement en cours, la liste des bases auxquelles il sera accédé peut évoluer. A ce jour deux familles de bases sont identifiées : les bases ERASME régionales et les bases Hippocrate-Décisionnel régionales également. Compte tenu de la nécessité de croiser des critères de nature « données de santé » avec d'autres critères, les dispositions existantes pour accéder à ce type de données seront appliquées (accès restreint aux médecins conseils en échelon médical). Les remontées de fichiers s'effectueront dans un premier temps par le système d'échange de fichiers sécurisé « Petra ». Une étude sera menée pour voir s'il sera nécessaire d'industrialiser ou non ce processus par la suite. L'élaboration et l'exécution de ces requêtes seront donc effectuées hors SI Vaccination Covid.

- Une étude en cours tend à privilégier la mise en place d'un ciblage plus général des personnes possiblement éligibles à la vaccination. Ceci permettra de couvrir tous les besoins (exemple : Notamment en cas de situation non connue - par exemple en phase 1 pour le critère de nature « socio professionnelle » - il sera nécessaire d'élargir la recherche par application des autres critères comme âge, facteur de comorbidité). Néanmoins, mêmes si les données sont déjà intégrées dans le SI, les invitations seront bien déclinées en fonction des phases (cf d) ci-dessous).

b. Le ciblage par les autres régimes

Le SI vaccination devant couvrir le champ inter-régimes, les données nécessaires des personnes ciblées relevant de la responsabilité des autres régimes devront être communiquées au SI vaccination. La norme d'échange ainsi que les spécifications des requêtes à exécuter par ces régimes leur seront communiquées en amont des opérations.

Les échanges de fichiers s'effectueront dans un premier temps par le système d'échange de fichiers sécurisé «Petra ». Une étude sera menée pour voir s'il sera nécessaire d'industrialiser ou non ce processus.

Pour ces populations, il sera nécessaire d'ajouter aux données restituées les coordonnées de contact permettant d'adresser à ces personnes les communications prévues (N° de téléphone portable, Email personnel valide, adresse postale décomposée/Adresse postale en bloc).

c. L'alimentation du SI Vaccin Covid par les requêtes de ciblage

Les données présentes dans les fichiers de ciblage seront injectées dans le SI vaccination par un traitement informatique de type batch, à déclenchement manuel avec l'application de règles de contrôle d'intégrité des données. Les éventuels rejets d'injection seront mis en réserve pour retraitement ultérieur. Les modalités de ce retraitement ne sont pas arrêtées à ce jour mais seront sans doute manuelles pour la première version ou ignorées.

Lors de l'injection d'un ciblage dans la base SI Vaccination, un dossier par patient unique est créé et un code unique est également généré. Ce code servira de clé pour permettre au PS de renseigner ensuite les données de la vaccination du patient via le téléservice, tout au long du cycle de la vaccination.

Il sera de la forme « AAA-AAA-AAA » ([A-Z]{3}-[A-Z]{3}-[A-Z]{3}).

Une notion de type de ciblage est également renseignée à la valeur « Automatique » pour différencier les patients issus de ce chargement initial de ceux issus d'une action du Professionnel de santé via le téléservice (cf § « Suivi du cycle de la vaccination par le téléservice »)

A noter qu'une même personne pourrait être concernée par plusieurs ciblages (ciblage initial puis ciblages complémentaires). Dans ce cas, elle ne sera enregistrée qu'une seule fois au premier ciblage et seule la liste de ses critères de ciblage sera alors actualisée.

d. L'envoi des invitations/bons

Une fois le ciblage enregistré en base SI vaccination, des notifications d'informations aux patients peuvent être émises via les canaux de communication sortante. Ces émissions sont régulées par une fonction batch de séquencement et de lissage qui vérifie quelle notification est à envoyer en fonction de la situation de chaque dossier patient en base et de la phase de vaccination en cours.

La fonction permet aussi de tenir compte de la capacité des outils gérant les canaux de communication sortante pour n'envoyer que le volume traitable de notifications par jour. Cette régulation peut également permettre de tenir compte d'une situation en capacité de vaccination inférieure au nombre de patients concernés par l'étape en cours.

=> Les outils de gestion des canaux de communication sortante sont ceux utilisés habituellement par l'assurance maladie pour ses communications vers les assurés. Aucun nouvel outil ou traitement n'est mis en œuvre pour le SI Vaccination (Centre De Notification, chaine éditique Esope, routeur mail et SMS OGC, …)

Pour la première phase de vaccination, il est acté de ne pas envoyer d'invitation, ni de rappel, dans la mesure où les personnes concernées par la phase 1 sont déjà bien identifiées (résidents en Ehpad ou USLD par exemple).

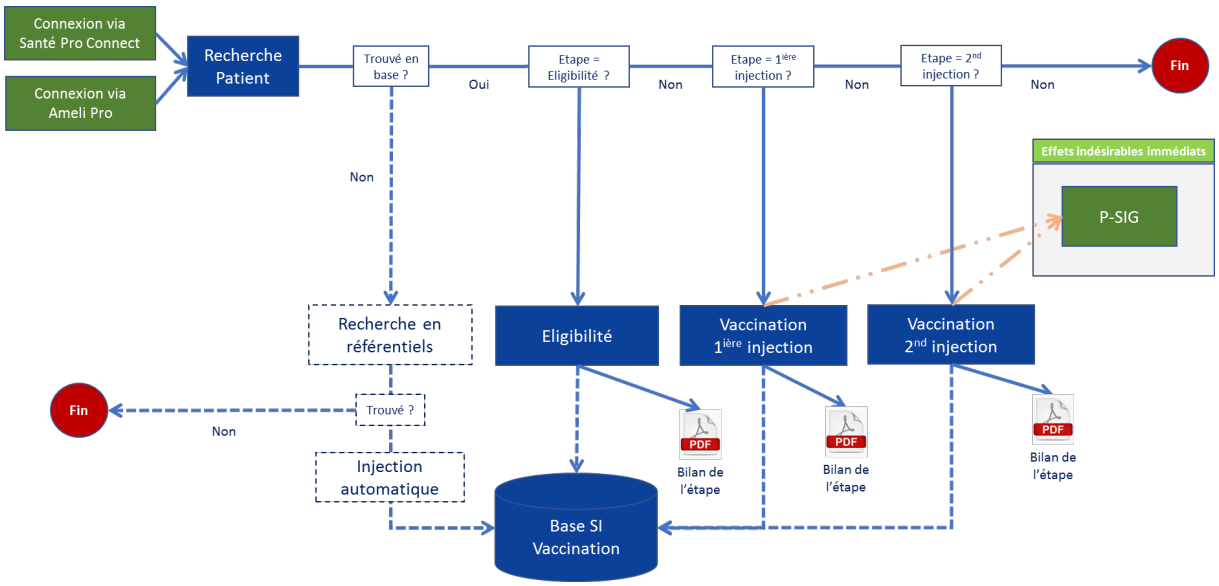
A ce jour, aucune fonction de relance/rappel des personnes invitées mais n'ayant pas initié leur cycle vaccinal (pas de consultation préalable réalisé) n'a été prévue. Pour rappel, le TLS mis en place n'a pas vocation à tenir un registre des personnes ayant refusé la vaccination.

e. Le ciblage par les professionnels de santé

L'Assurance Maladie ne pouvant cibler dans ses bases de données toutes les populations éligibles selon la décision ministérielle (ex : personne IMC supérieur à 30), les professionnels habilités à accéder au TLS pourront enregistrer manuellement leurs patients concernés.

L'enregistrement ne se fait que pour les patients souhaitant entrer dans le cycle vaccinal (consultation préalable).

2. Le suivi du cycle de la vaccination dans le TLS



Légende :

- En vert : externe au téléservice
- En bleu : les écrans du téléservice et la base de données
- En pointillée simple : traitement non visible de l'utilisateur
- En pointillée trait & double point : débranchement vers l'extérieur depuis le navigateur

a. Principe général

Le suivi du cycle de la vaccination sera réalisé par les professionnels de santé via un téléservice accessible depuis Ameli Pro. Ces professionnels accèderont au SI Vaccination lors de l'une des étapes du cycle vaccinal pour renseigner les données de suivi, dans l'ordre :

· En consultation pré-vaccinale pour renseigner l'éligibilité du patient à la vaccination

· En vaccination pour renseigner les différents rangs de la vaccination (première injection, seconde injection)

Une fois une étape renseignée, il ne sera plus possible de revenir sur la saisie effectuée. L'étape suivante sera alors automatiquement proposée en saisie. La dernière étape clôt les saisies.

A noter que ces différentes étapes peuvent être effectuées soit par un même professionnel de santé l'une à la suite de l'autre, soit par plusieurs professionnels de santé, en plusieurs fois. Chaque étape enregistrera bien le professionnel de santé l'ayant réalisée.

b. Les modalités d'accès au TLS

Le TLS est accessible via AmeliPro. Ainsi, seuls les professionnels de santé dotés de cartes CPS ou de eCPS pourront utiliser le téléservice.

A ce sous-ensemble de professionnel s'ajoutera des restrictions sur la catégorie et la spécialité du PS connecté, selon les indications du Ministère de la Santé en la matière. A ce jour ces restrictions n'étant pas connues, une liste par défaut est en cours d'étude.

La eCPS est un développement de l'ANS sous sa propre responsabilité (pas de documentation particulière fournie au titre du présent traitement).

c. La recherche d'un patient par un PS

Pour saisir les données des différentes étapes de la vaccination, le professionnel de santé accède au téléservice.

Une mention générale est ajoutée sur le 1er écran de recherche afin de rappeler aux PS que la recherche d'un patient et l'accès aux données est réservé au(x) professionnel(s) de santé assurant la prise en charge effective du patient pour la réalisation de la vaccination contre la Covid 19 (consultation préalable et vaccination). Toute recherche et accès illégitimes peuvent impliquer des sanctions.

Il accède alors à la recherche de patient en base en saisissant le code personnel porté sur l'invitation du patient.

En cas d'absence de code, le PS peut également rechercher le patient par son NIR, mais dans ce cas, il ne saura pas si ce patient a été ou non ciblé initialement.

Ceci permet de limiter les accès au SI Vaccination Covid, particulièrement les accès à des fins de recherche de patient ciblé. Une fois le patient trouvé, le PS accède directement à l'écran de saisie des données de l'éligibilité à la vaccination. Ainsi, seul le cas où le patient arrive avec son invitation et son code donne l'indication que celui-ci est bien présent en base.

Précision sur la rechercher par NIR : la fonction commence par rechercher en base SI Vaccination Covid. Dans le cas où le patient n'est pas retrouvé en base, la fonction enchaine de manière transparente pour l'utilisateur sur une recherche dans les référentiels inter-régimes de l'assurance maladie. Si le patient est trouvé alors l'utilisateur arrive directement en saisie des données de l'étape d'éligibilité sans aucune information sur le fait que le patient n'avait pas été ciblé. Il relève de la responsabilité du professionnel de santé en phase de consultation préalable de s'assurer que son patient, sans invitation ni code, fait bien partie des personnes concernées par la phase de vaccination en cours.

Précision sur le cas d'un patient non présent en base SI Vaccin Covid : ciblage manuel

Après une rechercher par NIR, dans le cas où un patient n'était pas présent en base, le système l'ajoute automatiquement en lui attribuant un type de ciblage « Manuel » afin de permettre d'identifier, en restitution de données, la différence d'avec un patient ciblé en amont.

Il n'est pas prévu à ce jour de permettre aux professionnels de santé d'ajouter des critères de ciblage lors de cette étape. Néanmoins la demande existe et devra être traitée dans une étape ultérieure, sans remettre en cause le principe exposé ci-dessus de transparence du ciblage initiale et en tenant compte des limites exposées au § « Données issues du ciblage » relativement à la finesse de ces critères. Il pourrait être envisagé par exemple de proposer systématiquement au professionnel de Santé d'enrichir les critères de ciblages par une saisie à choix multiples de critères compatibles avec les exigences exposées. Cela permettrait compléter les critères issus du schéma de priorisation de la HAS qu'il n'aurait pas été possible d'avoir initialement lors du ciblage (notamment les critères sociaux-économiques permettant d'identifier les groupes de professions les plus exposées).

d. La consultation préalable

Cette consultation a vocation à permettre l'information des patients éligibles (éligibilité AM ou déterminée par le médecin) sur le processus vaccinal, la détermination des éventuelles contre-indications etc. Elle aboutit à une prescription permettant au patient de bénéficier de la vaccination. Seules les données des personnes souhaitant entrer dans le processus vaccinal et donc disposer d'une telle prescription sont renseignées dans le TLS. En effet, ce TLS n'a pas vocation à suivre les refus de vaccination (une bulle d'information préciser au PS que les refus peuvent être consignés dans le dossier patient). C'est pour cette raison qu'il n'existe qu'une seule case à cocher actant de l'information et de l'accord pour entrer dans le processus (un refus n'a pas à être saisi).

Sur le processus organisationnel et les données saisies :

Une fois la recherche du patient effectuée, le professionnel de santé arrive directement sur l'écran de saisie des données de l'étape en cours.

Il visualise alors les informations du professionnel de Santé connecté (lui-même normalement : nom, prénom, identifiants AM). Il a accès également en visualisation aux données du patient (Nom, prénom, date de naissance, NIR, statut assuré ou ayant droit) et peut changer de patient (retour en recherche patient) si celui-ci ne correspond pas à la personne qui consulte (identito-vigilence).

Remarque : ces informations seront toujours présentes dans toutes les étapes et ne seront donc pas redécrites par la suite du document.

Dans le cas de l'éligibilité à la vaccination, deux cas de figure peuvent survenir lors de cette étape :

- le professionnel de santé connecté est bien celui qui réalise la consultation pré-vaccinal et qui délivre l'ordonnance de vaccination

- Le patient a déjà réalisé sa consultation pré-vaccinale mais celle-ci n'a pas été enregistrée dans le SI Vaccination Covid

Dans le premier cas, toutes les données d'identification du professionnel de santé qui effectue l'éligibilité du patient sont alors pré-alimentées à partir des données du professionnel de santé connecté et elles sont non modifiables. Dans le second cas, le professionnel de santé connecté peut quand même enregistrer l'éligibilité s'il le souhaite. Pour ce faire, il devra alors cocher « non » en regard de la phrase « Je suis le professionnel de santé qui délivre l'ordonnance». Il aura alors la possibilité d'enregistrer manuellement les informations portées sur l'ordonnance du patient et permettant d'identifier le professionnel de santé à l'origine de l'ordonnance. Les informations saisies seront alors purement indicatives, sans contrôle spécifique associé.

Dans les deux cas, les informations suivantes seront enregistrées :

- Professionnel de santé ayant réalisé l'éligibilité (n° RPPS et/ou n° AM, Nom, Prénom), et date de l'éligibilité

- Et le cas échéant le professionnel de santé ayant délivré la prescription s'il diffère du précédent (n° RPPS et/ou n° AM, Nom, Prénom) et la date de cette prescription

Il peut ensuite renseigner la date et l'heure de l'éligibilité (préaffichées à date et heure en cours mais modifiables) et cocher le ou les vaccins qu'il juge non préconisables (enregistrée à titre d'information et d'alerte pour le professionnel de santé qui réalisera la vaccination).

Enfin il devra cocher deux cases de manière volontaire :

- Une case indiquant que le patient éligible à la vaccination (ou son représentant légal) accepte d'entrer dans le processus de vaccination après avoir reçu toutes les informations nécessaires à son choix éclairé (un complément de description peut être consulté en cliquant sur un lien)

- Une case indiquant qu'il certifie avoir informé son patient (ou son représentant légal) sur le traitement de ses données et avoir pris connaissance des conditions de transmission des données (un complément de description peut être consulté en cliquant sur un lien)

Il valide ensuite ses saisies en cliquant sur le bouton « valider » ou les abandonne.

S'il les valide, il accède à un écran bilan lui récapitulant ses saisies :

- Identification du patient (Nom, Prénom, NIR, date de naissance, accord patient à « oui », code de l'invitation du patient

- Identité du professionnel de santé ayant déclaré l'éligibilité (n° RPPS et/ou n° AM, Nom, Prénom)

- date de l'éligibilité

- et le cas échéant identifié de professionnel de santé ayant délivré l'ordonnance s'il diffère du précédent (n° RPPS et/ou n° AM, Nom, Prénom) et la date de la prescription

Il peut alors le télécharger au format « pdf » pour impression et remise au patient ou enregistrement dans son propre SI. Ce « pdf » comprenant une mention I&L.

Depuis cet écran, il peut continuer sur l'étape suivante ou changer de patient.

e. La saisie des données en étape de Vaccination

Dans cette étape, le professionnel de santé connecté va pouvoir saisir les données propres à la vaccination. Ces données diffèrent selon les caractéristiques du vaccin.

Dans un premier temps, seuls des vaccins injectables en 2 injections sont gérés, mais par la suite, certains vaccins auront un mode d'administration différent et les données de la saisie devront alors être adaptées. A noter qu'à ce jour aucune donnée décrivant ces vaccins n'a été communiqué au projet.

La première donnée à saisir sera la dénomination du vaccin.

A terme, le professionnel de santé devra dès la première étape de vaccination, sélectionner le vaccin correspondant dans une liste déroulante. Pour la première version, un seul vaccin sera préaffiché.

Le stade en cours de la vaccination (en lien avec les caractéristiques du vaccin) seront préaffichés.

A chaque stade, le PS devra alors saisir les données en lien avec celui-ci.

Le premier vaccin étant injectable en 2 injections les stades seront « 1ière injection » puis « 2nd injection ».

A chaque stade le professionnel de santé devra saisir :

- le numéro de lot du vaccin

- le mode d'administration (préaffiché à injectable pour le premier vaccin)

- la date et heure de l'injection (préaffichées à date et heure en cours mais modifiables)

- la zone d'injection (choix entre « Bras gauche » ou « Bras droit »)

- la catégorie de lieu de vaccination en choisissant un lieu dans une liste déroulante (EHPAD, USLD, Résidence autonomie, Résidence service senior, Dans un autre établissement médico-social, Dans un autre établissement de santé, Au cabinet ou dans la structure d'exercice, Au domicile du patient, Autre)

- Un n° FINESS ou un n° SIRET facultatif

Enfin il devra cocher une case de manière volontaire :

- Une case indiquant qu'il certifie avoir informé son patient (ou son représentant légal) sur le traitement de ses données et avoir pris connaissance des conditions de transmission des données (un complément de description peut être consulté en cliquant sur un lien)

A noter qu'à tout moment, le professionnel de santé peut consulter le bilan de la ou des phases précédente en cliquant sur l'onglet de la phase.

Il valide ensuite ses saisies en cliquant sur le bouton « valider » ou les abandonne.

S'il les valide, il accède à un écran bilan lui récapitulant toutes les saisies effectuées jusque-là pour ce patient :

- Identification du patient (Nom, Prénom, NIR, date de naissance, accord patient à « oui », code de l'invitation du patient

- Identité du professionnel de santé ayant déclaré l'éligibilité (n° RPPS et/ou n° AM, Nom, Prénom)

- date de l'éligibilité

- et le cas échéant identifié de professionnel de santé ayant délivré l'ordonnance s'il diffère du précédent (n° RPPS et/ou n° AM, Nom, Prénom) et la date de la prescription

- Identité du professionnel de santé ayant réalisé le stade de la vaccination (n° RPPS et/ou n° AM, Nom, Prénom)

- Catégorie de lieu de vaccination, FINESS ou SIRET

- Données en lien avec le vaccin (nom du vaccin, n° de lot, stade de la vaccination, date de l'injection, heure de vaccination, mode d'administration, zone d'injection)

Il peut alors le télécharger au format « pdf » pour impression et remise au patient ou enregistrement dans son propre SI (mention I&L dans le pdf)

Depuis cet écran, il peut continuer sur l'étape suivante, changer de patient ou cliquer sur le bouton « Déclarer un effet indésirable immédiat ».

Dans ce dernier cas, un lien de type URL lui permet d'accéder directement via le navigateur de son poste au portail de signalement des effets de l'ANSM (P-SIG) pour le recueil des effets constatés.

Pour faciliter la saisie du professionnel de santé sur ce portail et éviter les erreurs de ressaisie, des informations concernant la vaccination du patient pourront également être communiquées en passage de contexte en version ultérieure :

- Patient : trigramme du nom d'usage, première lettre du prénom, Date de naissance, Sexe,

- PS vaccinateur : Nom, Prénom, Catégorie, N° de téléphone portable (sous réserve), Email professionnel (sous réserve), Identifiants du vaccin.

f. distribution de l'attestation certifiée de vaccination

A la suite de la phase vaccinale, le patient est positionné dans une salle d'attente pour une durée de 10 à 15mn et il lui est remis son attestation vaccinale à chaque phase de sa vaccination (si vaccin nécessite 2 doses par exemple). Cette attestation contenait jusqu'au 24 juin 2021 un code à barres de type 2D-DOC lui permettant de s'enregistrer dans le module carnet de l'application TousAntiCovid ou de présenter ce même code à barres à une autorité de contrôle, dans le cadre du pass sanitaire « événements ». Depuis le 24 juin 2021, le format du code à barres à évoluer pour prendre en compte le pass sanitaire européen et son format DCC.

3. Paiement des professionnels

Dans le cadre de la campagne de vaccination, il est prévu de rémunérer les professionnels de santé pour les actes effectués en consultation pré-vaccinal ainsi que lors de la vaccination. Pour ce faire, le SI Vaccin Covid communique, à la chaine de tarification des actes, un fichier permettant de procéder au calcul de tout ou partie des éléments constitutifs de cette rémunération. Les données exportées ne contiendront aucune information relative à la vaccination en elle-même mais uniquement des données permettant le calcul de la rémunération des professionnels de santé.

4. Base de pilotage interne Assurance Maladie (données dé-identifiées)

A des fins de pilotage et de surveillance du bon fonctionnement du SI Vaccination Covid, il est prévu la constitution d'une base de pilotage à chaud (base distincte de la base de gestion SI Vaccin Covid).

Cette base sera constituée dans un premier temps par des exports en annule et remplace de la base de production avec désidentification des données.

Dans un second temps des composants d'import / export pourraient prendre en charge des modalités d'alimentation plus complexes (agrégation, alimentation en delta, …).

A partir de cette base, des requêtes d'agrégation permettront de mettre à disposition des indicateurs de pilotage pour le suivi de la vaccination pour s'assurer du bon fonctionnement SI.

Ces indicateurs sont en cours de définition.

En exemple :

- Nombre de patient ciblés en automatique / en manuel par phase

o Répartition par département

- Nombre de patient ciblé / Nombre de patient invité / Nombre de patient en phase « Eligibilité » / nombre de patient en phase « Vaccination 1ière » …

Enfin, une restitution visuelle du résultat des requêtes d'agrégation sera possible sous la forme d'une IHM dédiée avec accès via habilitations et sécurisé par le système utilisé à L'assurance Maladie pour l'authentification et la gestion des habilitations (système Access Master / Passeport).

Il sera possible alors pour l'utilisateur de télécharger le résultat de la requête au format « csv » ou « xls ».

En interne AM, seules les personnes disposant d'un poste assurance maladie sécurisé et fonctionnant sur le réseau informatique de la Cnam pourront accéder à la visualisation des indicateurs, sous réserve quel leurs habilitations le leur permettent.

5**. Les usages par des destinataires**

a. Suivi de la couverture vaccinale

Les données exportées pour cette finalité seront totalement dé-identifiées et ne comporteront donc aucune information permettant d'identifier directement un patient (suppression du NIR, nom, prénom).

En première version, les données seront extraites et communiquées en annule et remplace. Ce mode de traitement pourra éventuellement évoluer vers un mode en différentiel en fonction des besoins.

Les données communiquées ne seront pas agrégées et comporteront :

- Les informations concernant le patient : Date de naissance, Sexe, Code postal commune de résidence, Code de la commune de résidence (sous réserve de faisabilité)

- Les informations en lien avec le ciblage : type de ciblage (automatique ou manuel), Code de la phase de ciblage, Codes ciblage (sous réserves exprimées au § « Données issues du ciblage »), Top invitation effectuée

- L'étape en cours de la vaccination

- Pour l'étape « Eligibilité » :

  - Identification du professionnel de santé (RPPS / AM), Nom, Prénoms, Catégorie,) ayant réalisé l'étape
  - Identification du professionnel de santé (RPPS / AM), Nom, Prénoms, Catégorie,) ayant rédigé l'ordonnance si différent du précédent
  - Vaccin non préconisé
  - Date et heure de réalisation

- Pour chaque étape « Vaccination » :

  - Identification du professionnel de santé (RPPS / AM), Nom, Prénoms, Catégorie,) ayant réalisé l'étape
  - Informations relatives au vaccin : nom, n° de lot, mode d'administration
  - Informations relatives à l'injection : zone d'injection
  - Informations relatives au lieu de vaccination : catégorie de lieu, code FINESS/SIRET

b. Suivi de l'efficacité vaccinale et envois à SPF (pseudonyme identique à SI-DEP)

Les données exportées pour cette finalité seront totalement dé-identifiées et ne comporteront donc aucune information permettant d'identifier directement un patient (suppression du NIR, nom, prénom).

En première version, les données seront extraites et communiquées en annule et remplace. Ce mode de traitement pourra éventuellement évoluer vers un mode en différentiel en fonction des besoins.

Les données communiquées ne seront pas agrégées et comporteront :

- Les informations concernant le patient : Identifiant pseudonymisé selon l'algorithme SI-DEP, Date de naissance, Sexe, Code postal commune de résidence, Code de la commune de résidence (sous réserve de faisabilité)

- Les informations en lien avec le ciblage : type de ciblage (automatique ou manuel), Code de la phase de ciblage, Codes ciblage (sous réserves exprimées au § « Données issues du ciblage »), Top invitation effectuée

- L'étape en cours de la vaccination

- Pour l'étape « Eligibilité » :

- Information relatives au professionnel de santé ayant réalisé l'étape (Catégorie, Lieu d'exercice)
- Vaccin non préconisé
- Date et heure de réalisation

- Pour chaque étape « Vaccination » :

- Information relatives au professionnel de santé ayant réalisé l'étape (Catégorie, Lieu d'exercice)
- Informations relatives au vaccin : nom, n° de lot, mode d'administration
- Informations relatives à l'injection : zone d'injection
- Informations relatives au lieu de vaccination : catégorie de lieu, code FINESS/SIRET

c. Alimentation SNDS et Health Data Hub
Cette partie de l'AIPD sera complétée ultérieurement, mais le mécanisme retenu sera celui prévu dans le cadre de l'arrêté du 10 juillet 2020.

d. Transmission des données à la base « séquestre »

L'ensemble des données figurant dans la base de données de VACCIN-COVID font l'objet d'un transfert vers un espace sécurisé de la DNUM afin de permettre l'information des personnes vaccinées en cas de risque nouveau. Ce mécanisme a fait l'objet d'un processus d'automatisation qui ne nécessite pas une intervention humaine.

Quels sont les supports des données ?

Les serveurs en charge de l'enregistrement des vaccinations réalisées par les professionnels de santé.

Principes fondamentaux

Proportionnalité et nécessité

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

Les finalités sont définies par le décret du 25 décembre 2020 et sont les suivantes :

1° L'organisation de la vaccination des personnes, l'identification des personnes éligibles à la vaccination au regard des recommandations vaccinales sur la covid-19 énoncées par le ministre chargé de la santé en application de l'article L. 3111-1 du code de la santé publique, l'envoi ou l'édition des invitations à la vaccination, la gestion de la prise de rendez-vous, l'enregistrement des informations relatives à la consultation préalable à la vaccination, à la gestion des rappels et au pilotage du dispositif ;

2° Le suivi de l'approvisionnement en vaccins et consommables, afin d'organiser leur mise à disposition dans les lieux de vaccinations ;

3° La production et l'envoi d'un récapitulatif des informations relatives à la vaccination, destiné à la personne vaccinée, établi par les professionnels de santé réalisant la vaccination ou par les personnels placés sous leur responsabilité ;

4° La mise à disposition de données pour permettre leur réutilisation à des fins de présentation de l'offre de vaccination, de surveillance de la couverture vaccinale, de mesure de l'efficacité et de la sécurité vaccinale, de pharmacovigilance, de production des indicateurs portant sur la qualité et la cohérence des statistiques produites dans le cadre de la campagne de vaccination, d'appui à l'évaluation de la politique publique de vaccination, et de réalisation d'études et de recherches ;

5° De permettre, en cas d'apparition d'un risque nouveau, conformément aux dispositions de l'article L. 1111-2 du code de la santé publique, la fourniture d'une information personnalisée aux personnes vaccinées et, le cas échéant, de les orienter vers un parcours de soins adaptés ;

6° D'assurer la prise en charge financière des actes liés à la vaccination.

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

Ce traitement est notamment fondé sur l'article 6-e du RGPD, le traitement est nécessaire à l'exécution d'une mission d'intérêt public. Quant à la collecte de données de santé, elle est autorisée au titre des articles 9-i pour ce qui concerne les motifs d'intérêt public dans le domaine de la santé publique et le 9- h quant aux fins de la médecine.

Par ailleurs, le présent traitement est créé par l'Etat et justifié par l'intérêt public. Conformément aux dispositions combinées des articles 31 II et 6 III de la loi informatique et libertés, un décret en Conseil d'Etat est donc requis.

Le décret qui a été soumis à l'avis de la CNIL et au Conseil d'Etat comporte l'ensemble des précisions requises par l'article 35 de la loi du 6 janvier 1978.

La mise en œuvre de ce traitement ne nécessite pas d'assouplissement des règles relatives au respect du secret médical et ne nécessite pas, dès lors, l'adoption d'une mesure législative dérogeant aux dispositions de l'article L. 1110-4 du code de la santé publique.

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 co-responsables de traitement « Vaccin Covid » ont veillé au strict respect du principe de minimisation des données collectées pour la réalisation des objectifs confiés et au respect de la confidentialité. Cette minimisation concerne aussi bien les données identifiantes que celles pseudonymisées pour permettre l'organisation et le suivi de la vaccination par les autorités sanitaires.

A ce titre, les professionnels de santé participant à la prise en charge n'auront pas accès au critère d'éligibilité de la personne invitée à se faire vacciner, lequel peut révéler dans certains cas, indirectement, son état de santé (ex. : ALD).

Ils n'auront accès qu'aux informations strictement nécessaires à la bonne prise en charge vaccinale de la personne concernée, à savoir : l'indication vaccinale qui aura été renseignée par un professionnel de santé lors de l'éventuelle consultation préalable, ainsi que les informations relatives aux éventuelles contre-indications (traitements en cours, allergies, etc.).

Pour leur strict besoin d'en connaître : un professionnel de santé n'a vocation à accéder qu'aux seules informations concernant la personne qu'il prend en charge, à partir du numéro figurant sur l'invitation au bénéfice de la vaccination que

la personne présentera, ou de son numéro d'inscription au répertoire national d'identification des personnes physiques. Les accès seront d'ailleurs sécurisés et tracés.

Par ailleurs, au sein du SI Vaccin Covid, les critères de ciblage ayant permis de cibler les patients pour servir la finalité « Suivi de l'efficacité vaccinale » ne seront pas directement présents en base. En effet, compte tenu du caractère sensible de cette information, celle-ci sera enregistrée sous forme de codification sans signification directe. La correspondance Codes / Libellés sera gérée séparément du SI Vaccination.

Les données sont-elles exactes et tenues à jour ?

L'exactitude des données collectées est assurée au moyen de contrôles classiques mis en place dans le TLS à a la saisie des données.
Aucun processus de mise à jour n'est en revanche prévu à ce stade, car les données sont par nature pérennes. Des modalités de purge des données à l'issue des durées de conservation sont en cours de définition. Une purge manuelle sera d'ores et déjà possible pour répondre aux demandes expresses d'oppositions des personnes ciblées par l'AM et ne souhaitant pas entrer dans le cycle de vaccination (purge au niveau national).

Quelle est la durée de conservation des données ?

Les données seront conservées par la CNAM en base active pendant 10 ans. Cette durée correspond à la durée de prescription des actions en responsabilité médicale. Un mécanisme d'archivage intermédiaire est en cours de définition

Les données contenues dans la base dite « séquestre » gérée par la DNUM, seront conservées pendant une durée de 30 ans. Une telle durée est justifiée pour les motifs suivants. Dans le contexte spécifique que représente la vaccination contre la Covid 19, à savoir une vaccination de masse des populations contre un virus sur lequel la communauté scientifique n'a encore que peu de recul et avec des vaccins développés à l'aide de technologies nouvelles, il paraît indispensable de prendre un maximum de précautions quant à la conservation de la traçabilité sur le long terme des informations relatives aux actes de vaccination réalisés auprès de chacun des patients.

En effet, les expériences passées sur des cas de crises liés à des produits de santé ont montré la difficulté de mettre à disposition des patients potentiellement exposés à un risque au cours de leur vie, les informations nécessaires pour leur permettre d'entreprendre les démarches adéquates en termes de suivi médical et/ou le cas échéant de recours auprès des organismes pouvant leur apporter un support et/ou une indemnisation (Office National d'Indemnisation des Accidents Médicaux en particulier), avec les conséquences dramatiques qu'on peut imaginer pour ces personnes et leurs proches.

Dans ce contexte, et afin d'éviter de se trouver confronté à une telle situation en cas de survenue d'effets indésirables à long terme, il est envisagé de conserver sur une durée de 30 années un socle de données personnelles strictement nécessaires à l'identification des patients potentiellement exposés à un risque qui apparaîtrait et serait identifié plusieurs années après la vaccination contre la Covid-19, afin d'être en mesure de les contacter y compris de nombreuses années après l'administration du vaccin, pour leur faire savoir, si nécessaire, qu'ils ont été exposés à un risque. A ce titre, sont concernées les données suivantes :

Données d'identification du patient, dont son NIR individu ;

Données relatives aux vaccins injectés : nom du vaccin, n° de lot, date des injections

A l'occasion de l'apparition d'un risque nouveau lié à un vaccin ou un lot, un accès à ces données sera autorisé afin que les personnes ayant été vaccinées et concernées par le risque soient identifiées pour recevoir une information individuelle et adaptée.

Une conservation de ces données sur une longue période est justifiée dans la mesure où l'apparition de risques nouveaux peut avoir lieu plusieurs dizaines d'années après un acte ou l'administration d'un produit. En outre, il peut être identifié sur la génération suivante, ainsi que ce fut le cas avec l'administration du distilbène aux femmes enceintes dont les effets sont apparus sur leurs enfants. C'est pour cela, par exemple, que la durée de conservation des données relatives à la pharmacovigilance, dans la banque nationale de pharmacovigilance (BNPV), est de 70 ans.

Dans ces conditions et afin de permettre à cette base de données de remplir sa finalité, une durée de conservation longue est justifiée. Par ailleurs, la gestion de cette base sera confiée à la DNUM, comme « tiers de confiance » sous-traitante de la DGS, afin de garantir la conservation de ces données dans des conditions de sécurité et d'intégrité optimales. Ces données seront ainsi hébergées chez OVH (certifié hébergeur de données de santé et labellisé SECNUM CLOUD), dont l'accès sera sécurisé par un bastion. La base de données est quant à elle chiffrée et sauvegardée pour en assurer l'intégrité. Un système d'authentification forte est en place pour l'accès aux données. Toutes les opérations font l'objet d'un mécanisme permettant de tracer les actions sur les données.

Mesures protectrices des droits

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

Les personnes concernées sont informées de diverses manière.

D'abord par une information générale, grâce à la publication du décret au journal officiel, ainsi que par la publication sur le site web du ministère de la santé et sur celui de l'assurance-maladie d'une mention complète d'information *:*

: https://solidarites-sante.gouv.fr/ministere/article/donnees-personnelles-et-cookies

https://www.ameli.fr/mention-information-si-vaccin-covid

Puis par une information individuelle :

- Au moment de la saisie des informations dans le SI :
    - Information à destination des patients par les PS (case à cocher dédiée) ;
    - Information à destination des PS dans le TLS (case à cocher) ;

- Pour les résidents en EHPAD : un guide a été adressé par le ministère de la santé à l'ensemble des directeurs d'EHPAD pour leur rappeler la nécessité d'informer les personnes candidates à la vaccination et la mention d'information leur a été communiquée ;

- Par la mention suivante figurant sur invitation/bon :

« L'envoi de cette invitation s'inscrit dans le cadre du traitement de données dénommé « SI Vaccin Covid » mis en œuvre par l'Assurance Maladie et la Direction Générale de la Santé. Ce traitement de données a pour finalité d'assurer l'organisation, la traçabilité et le suivi de la vaccination contre la Covid-19. Conformément aux dispositions relatives à la protection des données personnelles, vous disposez d'un droit d'accès, de rectification et de limitation aux données qui vous concernent, ainsi que d'un droit d'opposition sur une partie du traitement. Ces droits s'exercent auprès du Directeur de votre caisse d'assurance maladie de rattachement en contactant le ou la délégué(e) à la protection des données. Pour en savoir plus sur le traitement de vos données, rendez-vous sur le site d'information ameli.fr. »

- Par la mention suivante figurant sur les supports disponibles :

« L'organisation, la traçabilité et le suivi de la vaccination contre la Covid-19 nécessitent la mise en œuvre d'un traitement de données dénommé « SI Vaccin Covid » par l'Assurance Maladie et la Direction Générale de la Santé. Conformément aux dispositions relatives à la protection des données personnelles, vous disposez d'un droit d'accès, de rectification et de limitation aux données qui vous concernent, ainsi que d'un droit d'opposition sur une partie du traitement. Ces droits s'exercent auprès du Directeur de votre caisse d'assurance maladie de rattachement en contactant le ou la délégué(e) à la protection des données. Pour en savoir plus sur le traitement de vos données, rendez-vous sur le site d'information ameli.fr. »

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

Le traitement des données n'est pas fondé sur le consentement, mais sur l'intérêt public.

Les personnes restent libres d'entrer dans le circuit de vaccination mis en place et de se faire vacciner contre la Covid-19.

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

Le droit d'accès s'exerce auprès du directeur de l'organisme d'assurance maladie de rattachement de la personne concernée (professionnel de santé ou personne vaccinée), dans les conditions prévues aux articles 15, 16 et 18 du même règlement.

Le droit à la portabilité n'est pas applicable.

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

Le droit de rectification s'exerce auprès du directeur de l'organisme d'assurance maladie de rattachement de la personne concernée, dans les conditions prévues aux articles 15, 16 et 18 du même règlement.

Le droit à l'effacement ne s'applique pas au présent traitement (art. c du 3 de l'article 17 RGPD).

Une fonctionnalité existe sur le compte ameli pour saisir directement le DPO de son organisme

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

Droit de limitation s'applique dans les mêmes conditions que le droit d'accès et de rectification.

Le droit d'opposition : Les personnes dont l'éligibilité a été déterminée en amont par les organismes obligatoires de l'Assurance Maladie et qui ont été invitées (ou informées de cette éligibilité particulière) ont la possibilité de s'opposer au traitement de ces données tant qu'elles ne sont pas entrées dans le parcours vaccinal, c'est-à-dire tant qu'elles n'ont pas bénéficié d'une consultation préalable à la vaccination / tant qu'un professionnel de santé concourant à la vaccination n'a pas .

En effet, l'article 5 du décret prévoit bien que l'opposition s'applique « suite à l'identification des personnes éligibles à la vaccination par les organismes des régimes obligatoires d'assurance maladie ».

L'interprétation de la portée de cette disposition est que le droit d'opposition trouve à s'exercer après réalisation des opérations de ciblage et envoi de l'invitation aux personnes.

En effet, d'un point de vue de santé publique : Cette invitation est à la fois le moyen d'information quant à la présence dans la base (information au sens RGPD), mais surtout une information de santé essentielle pour la décision de la personne quant à la vaccination.

Cette position est en cohérence avec l'avis de la Cnil en 2009 sur le vaccin H1N1 et avec la position du Conseil d'Etat au sein du décret n°2015-390 du 3 avril 2015 qui exclut le droit d'opposition pour les traitements de l'Assurance Maladie comprenant la finalité prévention. Cette position s'inscrit plus largement dans les mécanismes d'absence d'opposition aux messages de prévention de l'Assurance Maladie qui ne constituent aucunement de la prospection et qui présentent un intérêt public indéniable.

Par ailleurs, Si nous appliquons une opposition « à la source » alors le responsable de traitement devrait garder des données de personnes pour empêcher un hypothétique envoi d'une invitation nous obligeant à gérer une liste d'opposition éventuelle assimilable à une liste de personne refusant par principe la vaccination. Il faut souligner que nous nous retrouverions alors à tenir indirectement une liste des personnes refusant la vaccination alors même qu'elles se sont peut-être même pas dans le SI Vaccin covid pour pouvoir gérer les opérations progressives de ciblage en fonction des recommandations. Cette liste serait plus impactante sur la vie privée que la réception d'un courrier portant un message dans l'intérêt à la fois individuel de la personne et de santé publique.

- ⇨ Dans le cas où les personnes exercent leur droit d'opposition après invitation, les données sont supprimées.

Par ailleurs, les personnes qui sont entrées dans le parcours vaccinal peuvent, à tout moment, s'opposer à la transmission de leurs données à des fins de recherche à la plateforme des données de santé « Health Data Hub » et à la Caisse nationale de l'assurance maladie.

Comment exercer ses droits ? Ces droits s'exercent sur demande écrite adressée soit au Directeur de l'organisme de rattachement (CPAM) soit au Délégué à la Protection des Données de la CNAM, soit sur l'espace prévu à cet effet du compte « ameli » de la personne.

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

Une convention de sous-traitance comportant des clauses RGPD est élaborée avec chaque sous-traitant afin de garantir que le sous-traitant présente des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à répondre aux exigences du RGPD et de la LIL.

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

Aucun transfert hors de l'Union européenne n'est réalisé dans le cadre de ce traitement.

Risques

Accès illégitime à des données

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

- IvP01.02 - Perte de chance dans le parcours de soins,
- IvP01.04 - Diffamation donnant lieu à des représailles physiques ou psychiques
- IvP02.01 -Perte de temps pour réitérer des démarches ou pour attendre de les réaliser
- IvP02.04 -Paiements non prévus
- IvP02.07 - Spams / messages non sollicités avec impacts sur une situation confidentielle (grossesse, traitement)
- IvP02.12 -Problème financier de longue durée
- IvP03.01 -Contrariété par rapport à l'information reçue, demandée, qualité du service,
- IvP03.02 - Perte de maîtrise sur ses données,
- IvP03.03- Sentiment d'atteinte/intrusion dans sa vie privée (sans préjudice réel et objectivable),
- IvP03.05 -Affectation psychologique mineure de type diffamation, réputation,
- IvP03.06 -Difficultés relationnelles avec l'entourage personnel comme professionnel,
- IvP03.10 -Chantage, harcèlement, cyberbullying, intimidation en ligne,

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

- Un usager (dont l'ID FranceConnect n'est pas réconcilié) saisit aléatoirement des NIR afin de récupérer des attestations ne le concernant pas
- Un usager saisit le NIR de ses proches après une authentification FC réusie afin de récupérer leurs NIRs
- Un agent curieux interroge le Téléservice Attestation Agent afin de vérifier l'état de vaccination de ses connaissances ou de VIP
- Un PS fournit par erreur l'attestation d'un vacciné à la mauvaise personne (confusion en centre de vaccination - confusion très probable au sein d'une même famille)
- Un administrateur prend connaissance volontairement ou involontairement, des données contenues dans VACCO
- Le flux de requête sur VACCO est intercepté par une personne malveillant externe ou interne
- Un agent interne, en charge du contrôle ou la gestion des contestations divulge les données contenues dans VACCO.
- Un administrateur divulgue les données contenues dans VACCO.
- Un attaquant anti-vaccin exploite une vulnérabilité du SI, fait une élévation de privilèges, s'introduit dans VACCO, et prend connaissance de la base de données.
- Un agent maladroit fournit par erreur l'attestation d'un assuré à un autre
- Une erreur de saisie engage l'envoi de l'invitation à la mauvaise personne
- Divulgation des données personnelles réelles utilisées en recette
- Les traces contiennent des données métier personnelles dont la consultation porte atteinte à la confidentialité des données

- Un assuré reçoit un mail de phishing et communique des données à caractère personnel (bancaire, santé, etc)
- Un attaquant qui récupère des identifiants FranceConnect, récupère les attestations vaccinales de ces usagers
- Un professionnel de santé requête l'application pour prendre connaissance des données relatives à un VIP puis les divulgue auprès de la presse
- Un professionnel de santé consulte l'application pour prendre connaissance des données relatives à un proche
- Un administrateur malintentionné consulte les données d'un VIP puis les divulgue auprès de la presse
- Un administrateur malintentionné consulte les données d'un proche sans justifier du besoin d'en connaitre
- Un attaquant externe exploitant des failles techniques accède à la base de données et divulgue des données sur la vaccination / Un attaquant exploite une vulnérabilité logicielle ou un défaut de conception de l'exposition internet de VacSi et prend connaissance aléatoirement des données de vaccination
- Un attaquant usurpe le compte d'un PS et prend connaissance des données de vaccination
- Un attaquant usurpe le compte d'un administrateur et prend connaissance des données contenues dans la base
- Un professionnel de santé possédant des droits utilisateur vend des données confidentielles patients
- Un administrateur malintentionné de l'Assurance Maladie habilité sur VacSI vend les données contenues dans la base
- Un attaquant réalise une campagne d'ingénierie sociale auprès de PS habilité sur VacSI et récupère des données de vaccination
- Les données d'adresse et de contact des patients assurés de la CNMSS sont renseignées et mises en visibilité dans les fiches patient
- Erreur de saisie de destinataire lors de l'envoi de mail contenant des données de ciblage issues des autres régimes ou de l'AM à destination de VacSI
- Absence de purge de données entrainant une atteinte à la confidentialité par un utilisateur n'ayant plus le droit d'en connaitre
- Un attaquant intercepte les flux d'échange entre VacSI et les autres composantes du SI (facturation, pilotage, comm sortante, Dnum, SPF) et prend connaissance aléatoirement des données en transit
- Un agent Assurance Maladie intercepte de façon malveillante un flux réseau ou accède aux serveurs par lesquels les fichiers transitent et prend connaissance aléatoirement des données de vaccination
- Un PS partage avec ses salariés administratifs son compte AméliPro ou ProSantéConnect. Ces derniers accèdent à de la donnée de santé portant atteinte à la confidentialité
- Le PC portable d'un agent vaccinateur est volé, les bilans de vaccination exportés au format PDF et stockés dans le poste sont récupérés
- Un attaquant exploite les vulnérabilités de l'URL exposée sur internet (hors AmeliPro) pour la connexion ProSantéConnect. Il usurpe un compte et accède aux données de vaccination.
- Un attaquant (interne ou externe) détourne l'API de lecture Dataset afin d'aspirer toutes les données de la BDD Vaccin Covid
- Une application tierce interne détenant une liste de NIR appelle l'API de Gestion Attestation et réussit à récupérer les attestations vaccinales correspondant à la liste de NIR
- Un PS fournit par erreur l'attestation d'un vacciné à la mauvaise personne (confusion en centre de vaccination - confusion très probable au sein d'une même famille ou avec des homonymes)
- Les données techniques (traces notamment) remontent des données personnelles de vaccination.

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

- Attaquant,
- Administrateur mal intentionné,
- Un professionnel de santé trop curieux,
- Un professionnel de santé avide d'argent,
- Agent de l'assurance-maladie,
- Un professionnel de santé ne respectant pas les principes de confidentialité,
- Un cambrioleur/voleur

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

- M1.01- Redondance des liens réseaux de l'Assurance Maladie
- M1.09- Traçabilité BASTION : solution de supervisation des accès administrateurs
- M1.12 - Traces des actions au sein de l'application (consultation / modification / suppression)
- M1.13 - Authentification forte pour accéder à VacSI
- M1.14 - Session Timeout (1h par exemple)
- M1.15 - Protection brute force AmeliPro (Temporisation)
- M1.16 - Traces des accès à l'application (réussite et échecs d'authentification)
- M1.17 - Chiffrement des flux d'envoi de données vers les partenaires par TLS
- M1.18 - Chiffrement des fichiers de suivi
- M1.25- Mises à jour de sécurité régulières des logiciels et composants d'infrastrutures et applicatives (Processus de patch-management)
- M1.26 - Chiffrement des flux d'alimentation de VacSI depuis le SI Ciblage (TLS)
- M1.27 - Chiffrement des fichiers de ciblage (AES 256)
- M1.29 - Chiffrement des flux d'échange entre VacSI et le SI Rémunération(TLS)
- M1.30 - Chiffrement applicatif des données en Base
- M1.31 - Authenfication forte pour les accès administrateurs
- M1.32 - Ne pas remonter les adresses des assurés de la CNMSS dans VacSI
- M1.33- Ne pas afficher le régime des assurés aux PS
- M1.34- PETRA : solution sécurisée de partage de fichiers
- M1.35 - Purge fréquente et automatisée des données en base (cf. Durée de conservation déclarée à la CNIL)
- M1.36 - Chiffrement des flux d'envoi de données vers les partenaires par TLS (DNUM et SPF pour le MVP)
- M1.37 - Chiffrement des fichiers de suivi (AES 256)
- M1.38 - Chiffrement des flux d'échange entre VacSI et la Comm' sortante (TLS)
- M1.40 - Mise en place d'un jeu de données fictives pour les tests le cas éhéant, dépersonnalisation des données réelles utilisées pour les tests
- M1.41 - Traçabilité des actions sur les environnements hors production hébergeant de la donnée réelle
- M1.42 - Contrôles d'accès et gestion des habilitations sur les environnements hors production hébergeant de la donnée réelle
- M1.43 - Séparation des environnements de test VacSI des autres espaces projet (Cloisonnement des environnements de recette par projet)
- M1.44 - Infrastructures de sécurité Réseau (F5, HA Proxy, etc, etc.)
- M1.45 - Mises à jour de sécurité régulières des composants de sécurité Réseau (Processus de patchmanagement HA Proxy et F5)
- M1.46 - Contrôle d'accès (Authentification & Habilitations) au puits de logs
- M1.47 - Recherche dans le TLS via le NIR ou le numéro d'invitation
- M1.50 - La recherche par le NIR ne permet pas de savoir si la personne a été ciblée
- M1.51 - Aucune action manuelle pour l'envoi des invitations à la vaccination
- M1.52 - Chiffrement applicatif des données BDD VACCO
- M1.53 - Authentification pour accéder à la base de rémunération VACCO
- M1.54 - Exposer le service QUID en https uniquement
- M1.55 - Autoriser uniquement les requêtes QUID sécurisées (SSL TLS ou HTTPS) sur VACCO.
- M1.56 - Authentification mutuelle entre QUID et VACCO (AuthApp)
- M1.57 - Modèle de droits - Habilitations spécifiques sur QUID
- M1.58 - traces des batchs (volumétrie, fréquences, erreurs d'exécution)
- M1.59 - Chiffrement des batchs d'envoi de données vers la base de Pilotage
- M1.60 - Tracibilité QUID
- M1.67 - Sécurité FranceConnect
- M1.73 - Chiffrer les flux entre le TLS Vaccin Covid et l'API de Gestion
- M1.74- Chiffrer les flux entre l'API de Gestion Attestation et l'API de Lecture Dataser
- M1.75 - Chiffrer les flux entre l'API de Lecture Dataset et la Base de données Vaccin Covid
- M1.76- Authentifier le TLS Vaccin Covid auprès de l'API de Gestion
- M1.77 - Authentifier l'API de Gestion Attestation auprès de l'API de Lecture Dataset
- M1.78 - Authentifier l'API de Lecture Dataset auprès de la Base de données Vaccin Covid
- M1.79 - Mettre à jour régulièrement les composants participant à la génération d'attestation vaccinale
- M1.80 - Authentifier tous les appels / accès à l'API de Lecture Dataset
- M1.81 - Définir strictement les seules données auxquelles l'API Lecture Dataset a accès (Dataset uniquement) mettre en place des scopes de données
- M1.82 - Mettre en place une gestion des autorisations sur les données (scopes de données) de la BDD Vaccin Covid

- M1.83 - Utiliser la brique d'API Management afin que celle-ci gère les droits et autorisations sur toutes les API participant à la génération d'attestation
- M1.84 - Authentifier tous les appels / accès à l'API de Gestion Attestation
- M1.85 - Mettre en place une gestion des autorisations sur l'API de Gestion Attestation
- M1.92 - Authentifier les accès au Téléservice Attestation Agent
- M1.93 - Mettre en place une gestion fine des habilitations sur le Téléservice Agent
- M1.94 - Limiter les accès des Agents aux seules données des Assurés de leur caisse (et les caisses déléguées dans le cadre de TRAM)
- M1.95 - Tracer tous les accès et actions sur le téléservice Attestation Agent
- M1.97 - Limiter le nombre d'appel du Téléservice Attestation Patient par @IP source
- M1.98 - Respecter les bonnes pratiques de développement OWASP
- M1.99 - Mettre en place un processus de rotation des clés
- M1.100 - Mettre en place une infrastructure de gestion de clé (HSM)
- M1.102 - Limiter l'accès aux traces de sécurité aux seules personnes justifiant du besoin d'en connaitre
- M1.103 - Ne pas remonter / occulter les données identifiantes dans les traces métier (Elastic)
- M2.05 - Contrat de travail de l'Assurance Maladie
- M2.09 - Plan de sensibilisation des PS
- M2.10 - CGU
- M2.12 - Serment de confidentialité du PS
- M2.13 - Communiquer le mot de passe PETRA via un autre canal que celui d'envoi du lien
- M2.14 - Respect de la politique de mot de passe
- M2.15 - Rappel de suppression des données
- M2.16 - Plan de sensibilisation des agents à la SSI
- M2.19 - Conventions entre l'AM et les instances recevant des données de VacSI
- M2.20 - Pas de données métier dans les traces applicatives et systèmes
- M2.23 - Processus continu d'analyse des traces de VacSI par le SOC de l'AM
- M2.24 - Sensibilisation des agents au RGPD
- M2.29 - Contrôle de la conformité des traitements par la MEC (Cnam)
- M2.31 - Contractualisation avec le sous-traitant
- M2.32 - Ajouter un critère de recherche pour accéder au dossier de vaccination (date de naissance, nom patronymique par exemple)
- M2.33 - Processus documenté de revue des accès (comptes, habilitations)
- M2.35 - CGU outil de pilotage QUID
- M2.38 - Sensibilisation des PS ou Agents en centre de vaccination
- M2.39 - Vérifier que le demandeur est bien celui qu'il prétend être
- M2.41 - Pas de données de santé ayant permis le ciblage dans la base
- M2.42 - Pas de restitution des critères de ciblages dans le TLS

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

Limitée

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

Négligeable

Modification non désirées de données

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

- IvP01.01 - Absence de prise en charge adéquate
- IvP01.02 - Perte de chance dans le parcours de soins
- IvP01.07 - Risque iatrogénique,
- IvP01.08 - Erreur médicale avec des impacts forts mais réparables,
- IvP01.09 - Affection physique majeure,
- IvP01.10 - Affection physique de longue durée,

- IvP02.01 -Perte de temps pour réitérer des démarches ou pour attendre de les réaliser,
- IvP02.04 -Paiements non prévus,
- IvP02.05 -Refus d'accès à des services administratifs /prestations
- IvP02.11 -Risque accru sur un déplacement à l'étranger (ex : problème de prise en charge), IvP02.14 -Perte d'emploi,
- IvP02.18 -Perte de preuve dans le cadre d'un contentieux,
- IvP03.02 - Perte de maîtrise sur ses données
- IvP03.03- Sentiment d'atteinte/intrusion dans sa vie privée (sans préjudice réel et objectivable)
- IvP03.08 - Sentiment d'atteinte aux droits fondamentaux (discrimination, liberté d'expression)

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

- Saisie dans l'application des données erronées sur le vaccin administré lors de la première vaccination ce qui impact la deuxième vaccination et le suivi sur la pharmacovigilance,
- Saisie erronée dans l'application concernant le vaccin à administrer ce qui entraine une erreur sur la prescription de vaccination et fait courir un risque sur la santé du patient,
- Saisie erronée dans l'application sur le vaccin administré lors de la deuxième vaccination le suivi sur la pharmacovigilance,
- Usurpation d'un compte PS et modifie les données des fiches patient entrainant des erreurs de vaccination -> rentre des données de première ou deuxième vaccination,
- Interception des fichiers de suivi et modifie leurs contenus avant de l'envoyer aux autorités publiques en charge du pilotage,
- Corrompt volontairement ou accidentellement la base de données VacSI provoquant des erreurs dans le processus de vaccination,
- Exploitation d'une vulnérabilité du SI, fait une élévation de privilèges, s'introduit dans la base VacSI et corrompt la base de données,
- Interception des fichiers de ciblage et modifie leur contenu avant de les envoyer à VacSI,
- Interception des données de ciblage échangées dans la plateforme DIFI et altération les exports vers VacSI.,
- Modification des informations PS dans les fiches patient ce qui entraine des erreurs de rémunération, Interception des flux de VacSI vers le SI facturation et modification de leurs contenus avant le des envoyer au SI facturation,
- Présence de données à caractère personnel non nécessaires au suivi de la vaccination,
- Une mauvaise intégrité de la base engage un suivi épidémiologique erroné entrainant des décisions nationales pouvant avoir un impact sur la santé des assurés,
- Altération des données de l'attestation pendant sa génération,
- Altération des données de vaccination,
- Altération des données de rémunération

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

- Attaquant,
- Administrateur mal intentionné,
- Un personnel de santé - prescripteur,
- Un personnel de santé - vaccinateur,
- Source non humaine (matériel défectueux)

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

- M1.09- Traçabilité BASTION : solution de supervisation des accès administrateurs
- M1.12 - Traces des actions au sein de l'application (consultation / modification / suppression)
- M1.13 - Authentification forte pour accéder à VacSI
- M1.14 - Session Timeout (1h par exemple)
- M1.15 - Protection brute force AmeliPro (Temporisation)
- M1.16 - Traces des accès à l'application (réussite et échecs d'authentification)
- M1.17 - Chiffrement des flux d'envoi de données vers les partenaires par TLS

- M1.18 - Chiffrement des fichiers de suivi
- M1.19 -Mécanisme de contrôle d'intégrité des fichiers de suivi (SHA 256 par exemple)
- M1.20 - Désensibilisation des données de pilotage (anonymisation / pseudonymisation)
- M1.21- Contrôle d'accès (Authentification + Habilitations) DIFI via Bastion
- M1.22- Chiffrement des données dans DIFI
- M1.23- Cloisonnement des espaces projets dans DIFI
- M1.24- Mécanisme de contrôle d'intégrité des fichiers de ciblage (SHA 256 par exemple) en entrée de VacSI
- M1.25- Mises à jour de sécurité régulières des logiciels et composants d'infrastrutures et applicatives (Processus de patch-management)
- M1.26 - Chiffrement des flux d'alimentation de VacSI depuis le SI Ciblage (TLS)
- M1.27 - Chiffrement des fichiers de ciblage (AES 256)
- M1.28 - Mécanisme de contrôle d'intégrité des fichiers de ciblage (SHA 256 par exemple)
- M1.31 - Authenfication forte pour les accès administrateurs
- M1.34- PETRA : solution sécurisée de partage de fichiers
- M1.36 - Chiffrement des flux d'envoi de données vers les partenaires par TLS (DNUM et SPF pour le MVP)
- M1.37 - Chiffrement des fichiers de suivi (AES 256)
- M1.38 - Chiffrement des flux d'échange entre VacSI et la Comm' sortante (TLS)
- M1.44 - Infrastructures de sécurité Réseau (F5, HA Proxy, etc.)
- M1.45 - Mises à jour de sécurité régulières des composants de sécurité Réseau (Processus de patchmanagement HA Proxy et F5)
- M1.48 - Limitation des champs libres
- M1.49 - Ciblage manuel par le médecin
- M1.53 - Authentification pour accéder à la base de rémunération VACCO
- M1.73 - Chiffrer les flux entre le TLS Vaccin Covid et l'API de Gestion
- M1.74- Chiffrer les flux entre l'API de Gestion Attestation et l'API de Lecture Dataser
- M1.75 - Chiffrer les flux entre l'API de Lecture Dataset et la Base de données Vaccin Covid
- M1.76- Authentifier le TLS Vaccin Covid auprès de l'API de Gestion
- M1.77 - Authentifier l'API de Gestion Attestation auprès de l'API de Lecture Dataset
- M1.78 - Authentifier l'API de Lecture Dataset auprès de la Base de données Vaccin Covid
- M1.79 - Mettre à jour régulièrement les composants participant à la génération d'attestation vaccinale
- M1.80 - Authentifier tous les appels / accès à l'API de Lecture Dataset
- M1.81 - Définir strictement les seules données auxquelles l'API Lecture Dataset a accès (Dataset uniquement) mettre en place des scopes de données
- M1.82 - Mettre en place une gestion des autorisations sur les données (scopes de données) de la BDD Vaccin Covid
- M1.83 - Utiliser la brique d'API Management afin que celle-ci gère les droits et autorisations sur toutes les API participant à la génération d'attestation
- M1.84 - Authentifier tous les appels / accès à l'API de Gestion Attestation
- M1.85 - Mettre en place une gestion des autorisations sur l'API de Gestion Attestation
- M1.92 - Authentifier les accès au Téléservice Attestation Agent
- M1.93 - Mettre en place une gestion fine des habilitations sur le Téléservice Agent
- M1.95 - Tracer tous les accès et actions sur le téléservice Attestation Agent
- M1.97 - Limiter le nombre d'appel du Téléservice Attestation Patient par @IP source
- M1.98 - Respecter les bonnes pratiques de développement OWASP
- M1.99 - Mettre en place un processus de rotation des clés
- M1.100 - Mettre en place une infrastrutre de gestion de clé (HSM)
- M2.05 - Contrat de travail de l'Assurance Maladie
- M2.07 - Procédure de sauvegarde partielle et incrémentale
- M2.08 - Procédure de restauration des sauvegardes
- M2.09 - Plan de sensibilisation des PS
- M2.10 - CGU
- M2.11 - Processus de vérification des données saisies par les PS
- M2.12 - Serment de confidentialité du PS
- M2.16 - Plan de sensibilisation des agents à la SSI
- M2.18 - Campagne nationale de sensibilisation au Phishing auprès de Assurés
- M2.19 - Conventions entre l'AM et les instances recevant des données de VacSI
- M2.23 - Processus continu d'analyse des traces de VacSI par le SOC de l'AM
- M2.24 - Sensibilisation des agents au RGPD
- M2.25 - Campagne nationale de communication sur la vaccination
- M2.26 - Obligations professionnelles

- M2.31 - Contractualisation avec le sous-traitant
- M2.32 - Ajouter un critère de recherche pour accéder au dossier de vaccination (date de naissance, nom patronymique par exemple)
- M2.33 - Processus documenté de revue des accès (comptes, habilitations)
- M2.38 - Sensibilisation des PS ou Agents en centre de vaccination

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

Importante

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

Importante

Disparition de données

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

- IvP01.01 - Absence de prise en charge adéquate,
- IvP01.02 -Perte de chance dans le parcours de soins,
- IvP03.06 - Difficultés relationnelles avec l'entourage personnel comme professionnel

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

- Un incident d'exploitation partiel survient sur l'infrastructure d'hébergement de l'Assurance Maladie,
- Un incident d'exploitation total survient sur l'infrastructure d'hébergement de l'Assurance Maladie,
- Suppression volontaire ou accidentelle d'une partition ou de la base de données VAC-SI

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

- Administrateur système mal intentionné,
- Administrateur de base de données mal intentionné,
- Un personnel de maintenance du datacenter,
- Un attaquant

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

- M1.01- Redondance des liens réseaux de l'Assurance Maladie
- M1.02 - Load Balancing de l'application VacSi (HA Proxy)
- M1.03 - Métrologie - Surveillance de la congestion du réseau de l'Assurance Maladie
- M1.04 - Dupliquer l'infrastructure de la Filière Digital sur un site géographique distinct du site principal
- M1.05 - Métrologie - Surveillance du comportement des application VacSI
- M1.06 - Métrologie - Surveillance du comportement des partitions informatiques hébergeant l'application VacSi
- M1.07 - Virtualisation des partitions hébergeant les composants logiciels de l'application
- M1.08 - Robustesse et scalabilité de la filière digitale
- M1.09- Traçabilité BASTION : solution de supervisation des accès administrateurs
- M1.10 - Procédure anti-DdoS orange
- M1.11 -Filtrage des adresses IP pouvant accéder au TLS VacSi
- M1.12 - Traces des actions au sein de l'application (consultation / modification / suppression)
- M1.13 - Authentification forte pour accéder à VacSI

- M1.14 - Session Timeout (1h par exemple)
- M1.15 - Protection brute force AmeliPro (Temporisation)
- M1.16 - Traces des accès à l'application (réussite et échecs d'authentification)
- M1.17 - Chiffrement des flux d'envoi de données vers les partenaires par TLS
- M1.18 - Chiffrement des fichiers de suivi
- M1.19 -Mécanisme de contrôle d'intégrité des fichiers de suivi (SHA 256 par exemple)
- M1.20 - Désensibilisation des données de pilotage (anonymisation / pseudonymisation)
- M1.21- Contrôle d'accès (Authentification + Habilitations) DIFI via Bastion
- M1.22- Chiffrement des données dans DIFI
- M1.23- Cloisonnement des espaces projets dans DIFI
- M1.24- Mécanisme de contrôle d'intégrité des fichiers de ciblage (SHA 256 par exemple) en entrée de VacSI
- M1.25- Mises à jour de sécurité régulières des logiciels et composants d'infrastrutures et applicatives (Processus de patch-management)
- M1.26 - Chiffrement des flux d'alimentation de VacSI depuis le SI Ciblage (TLS)
- M1.27 - Chiffrement des fichiers de ciblage (AES 256)
- M1.28 - Mécanisme de contrôle d'intégrité des fichiers de ciblage (SHA 256 par exemple)
- M1.29 - Chiffrement des flux d'échange entre VacSI et le SI Rémunération(TLS)
- M1.30 - Chiffrement applicatif des données en Base
- M1.31 - Authenfication forte pour les accès administrateurs
- M1.32 - Ne pas remonter les adresses des assurés de la CNMSS dans VacSI
- M1.33- Ne pas afficher le régime des assurés aux PS
- M1.34- PETRA : solution sécurisée de partage de fichiers
- M1.35 - Purge fréquente et automatisée des données en base (cf. Durée de conservation déclarée à la CNIL)
- M1.36 - Chiffrement des flux d'envoi de données vers les partenaires par TLS (DNUM et SPF pour le MVP)
- M1.37 - Chiffrement des fichiers de suivi (AES 256)
- M1.38 - Chiffrement des flux d'échange entre VacSI et la Comm' sortante (TLS)
- M1.39 - Authentification pour accéder à la base de pilotage
- M1.40 - Mise en place d'un jeu de données fictives pour les tests le cas éhéant, dépersonnalisation des données réelles utilisées pour les tests
- M1.41 - Traçabilité des actions sur les environnements hors production hébergeant de la donnée réelle
- M1.42 - Contrôles d'accès et gestion des habilitations sur les environnements hors production hébergeant de la donnée réelle
- M1.43 - Séparation des environnements de test VacSI des autres espaces projet (Cloisonnement des environnements de recette par projet)
- M1.44 - Infrastructures de sécurité Réseau
- M1.45 - Mises à jour de sécurité régulières des composants de sécurité Réseau (Processus de patchmanagement)
- M1.46 - Contrôle d'accès (Authentification & Habilitations) au puits de logs
- M1.47 - Recherche dans le TLS via le NIR ou le numéro d'invitation
- M1.48 - Limitation des champs libres
- M1.49 - Ciblage manuel par le médecin
- M1.50 - La recherche par le NIR ne permet pas de savoir si la personne a été ciblée
- M1.51 - Aucune action manuelle pour l'envoi des invitations à la vaccination
- M1.52 - Chiffrement applicatif des données BDD VACCO
- M1.53 - Authentification pour accéder à la base de rémunération VACCO
- M1.54 - Exposer le service QUID en https uniquement
- M1.55 - Autoriser uniquement les requêtes QUID sécurisées (SSL TLS ou HTTPS) sur VACCO.
- M1.56 - Authentification mutuelle entre QUID et VACCO (AuthApp)
- M1.57 - Modèle de droits - Habilitations spécifiques sur QUID
- M1.58 - traces des batchs (volumétrie, fréquences, eurreures d'éxecution)
- M1.59 - Chiffrement des batchs d'envoi de données vers la base de Pilotage
- M1.60 - Tracibilité QUID
- M1.61 - Chiffrement des flux d'envoi de données vers le SNDS
- M1.62 - Mécanisme de contrôle d'intégrité des fichiers à destination du SNDS (SHA 256 par exemple)
- M1.63 - Modèle de droits - Habilitations spécifiques sur Medialog+
- M1.66 - Protection Anti-DDoS d'orange en place à la Cnam
- M1.67 - Sécurité FranceConnect
- M1.69 - Dupliquer les données du dataset dans une base de données dédiée à la génération d'attesttion
- M1.70 - Limiter le nombre d'appels simultanés sur la BDD VacSI
- M1.71 - Limiter le nombre d'appels simultanés du TLS Vaccin Covid (depuis le même source)

- M1.72 - Mettre en place un capcha sur le TLS Vaccin Covid
- M1.73 - Chiffrer les flux entre le TLS Vaccin Covid et l'API de Gestion
- M1.74- Chiffrer les flux entre l'API de Gestion Attestation et l'API de Lecture Dataser
- M1.75 - Chiffrer les flux entre l'API de Lecture Dataset et la Base de données Vaccin Covid
- M1.76- Authentifier le TLS Vaccin Covid auprès de l'API de Gestion
- M1.77 - Authentifier l'API de Gestion Attestation auprès de l'API de Lecture Dataset
- M1.78 - Authentifier l'API de Lecture Dataset auprès de la Base de données Vaccin Covid
- M1.79 - Mettre à jour régulièrement les composants participant à la génération d'attestation vaccinale
- M1.80 - Authentifier tous les appels / accès à l'API de Lecture Dataset
- M1.81 - Définir strictement les seules données auxquelles l'API Lecture Dataset a accès (Dataset uniquement) mettre en place des scopes de données
- M1.82 - Mettre en place une gestion des autorisations sur les données (scopes de données) de la BDD Vaccin Covid
- M1.83 - Utiliser la brique d'API Management afin que celle-ci gère les droits et autorisations sur toutes les API participant à la génération d'attestation
- M1.84 - Authentifier tous les appels / accès à l'API de Gestion Attestation
- M1.85 - Mettre en place une gestion des autorisations sur l'API de Gestion Attestation
- M1.92 - Authentifier les accès au Téléservice Attestation Agent
- M1.93 - Mettre en place une gestion fine des habilitations sur le Téléservice Agent
- M1.94 - Limiter les accès des Agents aux seules données des Assurés de leur caisse (et les caisses déléguées dans le cadre de TRAM)
- M1.95 - Tracer tous les accès et actions sur le téléservice Attestation Agent
- M1.97 - Limiter le nombre d'appel du Téléservice Attestation Patient par @IP source
- M1.98 - Respecter les bonnes pratiques de développement OWASP
- M1.99 - Mettre en place un processus de rotation des clés
- M1.100 - Mettre en place une infrastrutre de gestion de clé (HSM)
- M1.101 - Vérifier la cohérence des données du triplet FC et NIR réconcilié ou saisi aux données dans la base Vaccin Covid et en cas d'incohérence rejeter la demande d'attestation
- M1.102 - Limiter l'accès aux traces de sécurité aux seules personnes justifiant du besoin d'en connaitre
- M1.103 - Ne pas remonter / occulter les données identifiantes dans les traces métier (Elastic)
- M2.01 - Procédure de test de coupure électrique, essais
- des groupes électrogènes
- M2.02 - Recette et bench de l'application VacSi avant la
- mise en production
- M2.03 - Renforcer la supervision de la filière digitale
- M2.04 - Certification Tiers III des centres d'hébergement
- M2.05 - Contrat de travail de l'Assurance Maladie
- M2.06 - Définir des SLAs sur VacSI
- M2.07 - Procédure de sauvegarde partielle et incrémentale
- M2.08 - Procédure de restauration des sauvegardes
- M2.09 - Plan de sensibilisation des PS
- M2.10 - CGU
- M2.11 - Process us de vérification des données saisies par les PS
- M2.12 - Serment de confidentialité du PS
- M2.13 - Communiquer le mot de passe PETRA via un autre canal que celui d'envoi du lien
- M2.14 - Respect de la politique de mot de passe
- M2.15 - Rappel de suppression des données
- M2.16 - Plan de sensibilisation des agents à la SSI
- M2.17 - Privillégier le compte Ameli (et comptes similaires des autres régimes) pour l'envoi de l'invitation
- M2.18 - Campagne nationale de sensibilisation au Phishing auprès de Assurés
- M2.19 - Conventions entre l'AM et les instances recevant des données de VacSI
- M2.20 - Pas de données métier dans les traces applicatives et systèmes
- M2.21 - Tenue d'un journal de bord de partage des comptes
- M2.22 - Contrat de travail des agents de l'AM et des partenaires (DNUM)
- M2.23 - Process us continu d'analyse des traces de VacSI par le SOC de l'AM
- M2.24 - Sensibilisation des agents au RGPD
- M2.25 - Campagne nationale de communication sur la vaccination
- M2.26 - Obligations professionnelles
- M2.27 - Procédure de gestion de droit d'opposition
- M2.28 - Démarche d'identito-vigilance

- M2.29 - Contrôle de la conformité des traitements par la MEC (Cnam)
- M2.30 - Saisie à posteriori des données de vaccination dans le TLS
- M2.31 - Contractualisation avec le sous-traitant
- M2.32 - Ajouter un critère de recherche pour accéder au dossier de vaccination (date de naissance, nom patronymique par exemple)
- M2.33 - Processus documenté de revue des accès (comptes, habilitations)
- M2.35 - CGU outil de pilotage QUID
- M2.36 - Processus documenté de revue des accès (comptes, habilitations) sur Medialog+
- M2.37 - CGU outil de pilotage Medialog+
- M2.38 - Sensibilisation des PS ou Agents en centre de vaccination
- M2.39 - Vérifier que le demandeur est bien celui qu'il prétend être
- M2.40 Existence d'autres canaux pour récupérer l'Attestation
- M2.41 - Pas de données de santé ayant permis le ciblage dans la base
- M2.42 - Pas de restitution des critères de ciblages dans le TLS

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

Importante

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

Négligeable

Plan d'action

Principes fondamentaux

Résumé des principaux évènements redoutés :

- Non-respect de la minimisation dans la collecte des données (2)
- Manquement à l'obligation d'information (PS / Patients) (2)
- Détournement des canaux de communication de la Cnam (ex: fausse campagne de communication amenant le patient à consulter un site web douteux...) (3)
- Perte d'intégrité des données entrainant un suivi faussé de la vaccination (3)
- Accès à des données sensibles Patients (2)
- Non-respect du droit d'opposition (2)
- Non-respect des délais de conservation des données (2)
- Détournement de finalité (2)
- Vol de l'invitation à la vaccination entrainant une perte de chance pour la personne ciblée (3)
- Accès non maitrisé aux applications internes Cnam (Ciblage) (2)
- Risque d'escroquerie

Mesures existantes ou prévues

Compte tenu du peu de temps pour élaborer une architecture matérielle et logicielle, un audit de code a été réalisé par les équipes de développement de la CNAM et l'ANSSI a également débuté, auprès de la CNAM, courant mai 2021, un accompagnement relatif à l'architecture technique.
Un test d'intrusion est en cours par le prestataire Wavestone
L'AIPD sera mise à jour de manière régulière

Risques

Plan d'action

- L'élaboration d'une cartographie globale des SI thématique COVID
- Des tests d'intrusion et audit de configuration
- Prolongement des actions d'accompagnement et une revue des audits par l'ANSSI
- Audit d'exposition des vulnérabilités sur Internet (service SILENE) par l'ANSSI
- Approfondissement de l'analyse des architectures techniques, avec prise en compte de l'administration système cible privilégié des attaques actuel.
- Consolidation des scenarios de risque opérationnel
- Compléter et actualiser de l'analyse des risques SI :
    - *Afin d'implémenter la couverture des mesures de sécurité indiquées dans la PSSI-MCAS, les scénarios opérationnels et le plan de traitement*
    - *Lors de l'ajout d'une nouvelle connexion avec un SI externe, d'une nouvelle partie prenante, d'une source de risque ou d'une nouvelle fonctionnalité*
- Renforcer les outils de supervision