Questionnaire d'évaluation de la sécurité et analyse d'impact
Outil SHIFT – intelligence artificielle lutte contre les fraudes

Référence locale du Qersi : xxxx

Version de l'analyse de risques locale			
Version	*Date*	*Rédacteur*	*Objet de l'évolution*
1.0			

CONFIDENTIEL

Fiche méthodologique d'utilisation

Point d'attention **:**

- *Le remplissage du Qersi implique pour les rédacteurs de se placer dans le scénario le plus défavorable afin de ne pas aborder les risques de manière minimale.*
- *Si le cahier des charges évolue, une révision du Qersi sera nécessaire.*

Le QERSI est l'élément central de la démarche de mise en conformité des traitements de données à l'ensemble des règles relatives à la protection des données (RGPD, loi dite informatique et libertés, etc.).

L'expertise menée au travers du QERSI peut permettre la réalisation d'un PIA au sens de l'article 35 du RGPD lorsqu'il est requis. Le DPO et le MSSI/RSSI peuvent toutefois demander toute autre documentation qu'ils pourraient juger utile pour mener l'analyse. Des démarches supplémentaires, et notamment l'obtention préalable de l'avis des personnes concernées ou de leurs représentants, peuvent être requis.

Qui complète le document : le demandeur métier du projet = maitrise d'ouvrage (avec l'aide de la maitrise d'œuvre (service informatique, services généraux ou autre, si nécessaire)

Où : réunion préparatoire au projet (maximum 1heure) : MSSI-DPO-MOA-MOE

Quand : suffisamment en amont du projet pour apporter les conseils nécessaires à la mise en œuvre sécurisée de chacun des projets

Comment : en répondant aux questions présentées dans le questionnaire

Pourquoi : permettre de cerner très rapidement les risques potentiels liés au projet afin de les intégrer dans la montée en charge de celui-ci, ainsi que respecter/intégrer les obligations inhérentes à la réglementation dite « Informatique et libertés » (exemples : RGPD / loi Informatique et libertés). Le QERSI ne bloque pas le projet mais le facilite.

Le MSSI et le DPO analysent ce dossier et soit le valident en l'état (ou après un éventuel échange avec la MOA), soit demandent une étude approfondie si nécessaire
NB :

- Le MSSI et le DPO n'ont pas le pouvoir de validation sur le traitement et sa mise en œuvre.
- C'est au responsable de traitement, in fine, que revient cette responsabilité sous les conseils avisés du MSSI et du DPO

SOMMAIRE

1 Renseignements généraux relatifs au projet

1.1 Contacts

	Réponses
Nom du projet	**Expérimentation SHIFT**
Acronyme si projet informatique (ex : PLEIADE)	**SHIFT**
Responsable du projet	[redacted]
Fonction du responsable du projet	[redacted]
Métier concerné (maitrise d'ouvrage)	**Lutte contre la fraude**
Maitrise d'œuvre (informatique, services généraux, ou autre service)	**Direction des affaires juridiques et de la lutte contre la fraude** **Direction de la gestion du risque - Pôle expertise statistiques et informationnel**
Administrateur de l'outil en cas de projet informatique (application, service, ou autre) *Facultatif*	**SHIFT Technology**
Date de mise en œuvre prévue de l'outil *Facultatif*	**Avril 2025**
Date de rédaction, rédacteur et contact	**18/08/2025** [redacted]

1.2 Présentation générale du projet

Finalités du traitement ou projet *(Définir les finalités du projet au regard de la loi informatique et libertés)*:

⚠ **Tout changement de la finalité doit faire l'objet d'une révision de l'analyse des risques**

Dans la perspective d'intensifier la capacité de l'assurance maladie à détecter des fraudes en réseau, la Cpam de Paris a signé, le 18/03/2025 et pour une durée de 1 an, une convention d'expérimentation avec la Cnam et la société prestataire SHIFT Technology. Cette dernière, forte d'une expérience sur la détection des fraudes dans le secteur des complémentaires santé, a été identifiée comme pouvant être sous-traitante dans la conception d'un nouvel outil de repérage des fraudes, abus et paiements à tort, par l'intermédiaire d'une intelligence artificielle

Une expérimentation est ainsi prévue sur le territoire parisien. SHIFT Technology va adapter sa solution ***HEALTHCARE FRAUD WASTE & ABUSE DETECTION*** pour que les équipes compétentes de la CPAM de Paris puissent détecter des suspicions de fraude, faute, abus et paiement à tort dans les facturations de matériel optique et/ou auditif.

Présentation sommaire du projet *(expliquer ce que fait le projet, détailler les objectifs du projet et décrire les principales fonctions du processus de traitement)*:

En complément des outils déjà employés pour la détection spécifique de ces atypies, et considérant que les objectifs fixés par la Caisse nationale en matière de lutte contre la fraude deviennent plus ambitieux, la CPAM de Paris souhaite :

- automatiser certains contrôles ;
- fiabiliser ses modalités de détection des suspicions de fraudes ;
- réduire les délais de détection des fraudes et en faciliter les investigations.

Un outil d'intelligence artificielle performant établi à l'aide d'algorithmes de "*machine learning*" (apprentissage automatique) permettrait une aide à la décision pour mieux identifier des scénarios de détection d'anomalies. L'objectif est une amélioration continue de la pertinence (affinage des scénarios existants / ajustements des seuils de sélection) à partir des qualifications (anomalie ou non) des équipes.
Cet outil devra réunir les prérequis suivant :

- ⇨ Technologie d'intelligence artificielle avec a minima une solution de "*machine learning*"
- ⇨ Expérience opérationnelle avec d'autres clients type mutuelles ou assurance
- ⇨ Capacité à absorber la charge de l'Assurance maladie *(pour Paris : 2,2M de bénéficiaires, 16 000 professionnels de santé, 700 établissements de santé)*
- ⇨ Respect des contraintes RGPD de l'Assurance Maladie
- ⇨ Interface ergonomique pour le client final (les agents du département de lutte contre la fraude, et plus spécifiquement ceux du pôle détection et investigation, et éventuellement les agents de la mission paiement à bon droits de la Direction comptable et financière)

- ⇨ Adaptabilité à tout type de public de l'Assurance maladie
- ⇨ Adaptation à tout type de remboursement (paiement en tiers payant et paiement directement à l'assuré) et si possible et en fonction des tests, détection des préjudices a priori.

SHIFT Technology va adapter sa solution **HEALTHCARE FRAUD WASTE & ABUSE DETECTION** aux contours et objectifs de l'expérimentation parisienne. Elle va spécifiquement développer une bibliothèque d'algorithmes d'apprentissage automatique permettant de détecter plus facilement les anomalies de facturation d'appareillage optique et/ou auditif (exemple : *paiement d'audioprothèses en grand nombre et en tiers payant alors que les bénéficiaires sont très jeunes, etc*).

Les équipes du département lutte contre les fraudes qualifieront alors les alertes détectées par l'outil pour indiquer sur la base des résultats obtenus s'il s'agit effectivement d'une anomalie. Parallèlement, SHIFT Technology améliorera continuellement la pertinence de sa solution par l'adjonction de nouveaux scénarios.

Y a-t-il une motivation particulière à ce projet : texte de Loi, Directive, Lettre Réseau, Autre ?

- ⇨ **Axe 5 de la COG 2023-2027** : Déployer une stratégie ambitieuse de lutte contre la fraude.
- ⇨ [redacted] programme national de lutte contre la fraude des prescriptions et des facturations d'audioprothèses
- ⇨ [redacted] contrôle de la conformité des pratiques professionnelles aux obligations de présentation de l'offre du "100% Santé optique"
- ⇨ **Expérimentation souhaitée par la Cnam et confiée à la Cpam de Paris** (*avant toute phase d'industrialisation si les résultats s'avèrent concluants*)
- ⇨ **Poids jusqu'alors conséquent des fraudes en matière d'audioprothèses et d'appareillages optiques.**

Précisez où se trouve la documentation (documentation en amont du projet : expression de besoin, note de cadrage, cahier des charges, spécificités fonctionnelles, suivi de projet, contractualisation, etc.)

L'ensemble des éléments est enregistré sur un espace dédié sur le serveur de la DAF-LCF.

1.3 Périmètre géographique

(Indiquer le plus grand)

☑ Interne à l'organisme *(commentaire facultatif)* ☐ Réseau Assurance Maladie *(préciser)* ☑ Autre : partenaires, PS, … *(préciser)*

- ⇨ Assurés et ayant-droit affilés au parisiens
- ⇨ Professionnels de santé France entière.

	Réponses
Nombre approximatif de personnes concernées *(personnes traitées par l'application et non pas utilisateurs de l'application)*	Près de 2,3 millions de personnes concernées au total : assurés sociaux parisiens et les professionnels de santé prescripteurs et les professionnels de santé exécutants (France entière)
Catégorie de personnes concernées *(assurés, professionnels de santé, salariés / agents, usagers employeurs, personnes mineures, autres)*	- 2,11 millions d'assurés parisiens - 3800 médecins ophtalmologues (France entière) - 1700 médecins ORL (France entière) - 100 000 médecins généralistes (France entière) - 44 000 centres d'optiques (France entière) - 7500 centres d'audioprothèses (France entière) - 1 229 centres de santé médicaux et polyvalents - 2900 orthoptistes (France entière)

2 Cas d'un projet informatique

2.1 Informations relatives aux données

Dans la colonne précisions, indiquer tout ce qui est de nature à éclairer le DPO et le MSSI au regard des risques et des besoins (*). Le remplissage de cette colonne est obligatoire.

(*) L'appréciation du DPO se fait surtout sur une justification du besoin / de la nécessité de collecte de la donnée au regard de la finalité.

	Précisions (détails et justifications)	***Commentaires DPO/MSSI***
Utilisation de données directement ou indirectement identifiantes *(nom, prénom, adresse e-mail, un identifiant, …)* *<u>Attention</u> : un identifiant peut paraitre neutre mais peut identifier de manière unique une personne*	**OUI** **• Identification des personnes (assurés et ayants droits)** [redacted] **• Identification du professionnel de santé exécutant ou prescripteur :** [redacted]	⇨ **Données pseudonymisées** [redacted] ⇨ **Dossiers pseudonymisées pour le numéro AM et le prénom du PS** ⇨ [redacted]

	Précisions (détails et justifications)	*Commentaires DPO/MSSI*
		[redacted]
Utilisation de données de santé *(cf. considérant du RGPD).* [redacted]	**OUI** ⇨ **Assurés et ayants-droits :** [redacted] ⇨ **Professionnel de santé :** [redacted]	⇨ **Nécessité pour le Prestataire de disposer :** - de l'ensemble des consommations de soins en lien avec la prescription optique ou audio (matériel optique ou audio, consultation et actes techniques ophtalmo, ORL ou médecin généraliste) - de l'ensemble des prestations autre qu'optique et audioprothèses à +/- 3 jours des dates de prescription de l'optique et de l'audioprothèse ⇨ **Nécessité pour le Prestataire** d'identifier les anomalies entre les différents actes exécutés sur un même ayant-droit ou plusieurs ayant-droit rattaché à un même assuré, ainsi que les anomalies au niveau des volumétries des actes effectués par PS - Transmission des codes de regroupement sans le code affiné/détaillé, excepté pour les prestations audio et optique - Les quantité d'actes effectués ou de produits vendus figurent en clair pour identifier les anomales statistiques.
Utilisation de données avec impacts financiers *(RIB, génération d'un paiement, …)*	⇨ **Assurés et ayants-droits :** [redacted]	⇨ **- Nécessité pour le prestataire d'identifier les banques** dont le taux de fraude constaté par Shift est supérieur à la moyenne. [redacted]

	Précisions (détails et justifications)	*Commentaires DPO/MSSI*
	⇨ **Professionnel de santé :** [redacted]	- Nécessité pour le prestataire d'identifier les anomalies liées à l'écart entre date de paiement et date de soins et d'utiliser la date de paiement pour la détection de doublons => La date de paiement de la prestation (mandatement) apparaîtra en clair. ⇨ **- Nécessité pour le prestataire d'identifier les banques** dont le taux de fraude constaté par Shift est supérieur à la moyenne. [redacted] - Nécessité pour le prestataire de disposer en clair du **numéro de facture** et de **lot**, ainsi que du **prix de l'acte audio** et/ou **optique** pour la détection de doublons.
Le projet utilisera le **NIR**	**OUI :** [redacted]	Donnée pseudonymisée
Données liées à **des infractions, condamnations, mesures de sûreté**	Non	
Données relatives à l'appréciation sur des **difficultés sociales des personnes**	**OUI** [redacted]	
Données relatives à des **mineurs**	**OUI :** [redacted]	

	Précisions (détails et justifications)	*Commentaires DPO/MSSI*
	[redacted]	
Données **biométriques**	Non	
Données **génétiques**	Non	
Données de **géolocalisation**	Non	
Données relatives à l'**appartenance syndicale**	Non	
Données relatives à la **vie sexuelle**	Non	
Données relatives aux **origines raciales ou ethniques**	Non	
Données relatives aux **opinions politiques, philosophiques ou religieuses**	Non	
Données relatives à la **sécurité** *(analyse de risque, mots de passe, failles de sécurité, etc.)*	Non	
Données relatives au **personnel** *(sanctions disciplinaires, condamnations, saisies sur salaire, etc.)*	Non	
Données **stratégiques** d'organismes	Non	
Données relatives aux suspicions de **fraudes**	Non	

	Précisions (détails et justifications)	***Commentaires DPO/MSSI***
Autres données *(à préciser)*	• Rattachement et droits d'assurance maladie Assurés et ayants-droits : [redacted] • Vie personnelle [redacted] • Vie professionnelle [redacted] • Données externes : données publiques du Répertoire Partagé des Professionnels intervenant dans le système de Santé (RPPS) (Ministère de la Santé), et Registre National des Entreprises de l'INPI (RNE).	• Données sur les droits transmis en clair pour cibler uniquement les assurés avec droits et pour reconstituer les familles. [redacted] • Possibilité d'identifier les ayants-droits de l'assurés, sans mention du lien familial • Spécialité du PS transmise en clair pour que le Prestataire identifie les anomalies entre la spécialité du PS et les soins prescrits ou exécutés [redacted] • Données intégrées par Shift • Pour le traitement de l'anomalie par les agents habilités = obligation de recrypter les données à l'aide d'un outil interne pour procéder aux investigations

Description des principales fonctions du processus de traitement

	Qui fait *(préciser profil métier, service ou organisme)*
Extraction et actualisation des données	Actualisation par quinzaine via le lancement d'une requête « presse-bouton » par : • Le Secteur statistiques de la CPAM de Paris • La statisticienne de la DAJ-LCF
Pseudonymisation des données	Service Application de la Cpam de Paris (au travers d'un outil conçu et hébergé en interne)
Dépôt et transmission des données	• Pour les données = compétence du Service Application de la Cpam de Paris (dépôt par quinzaine via l'outil dédié [redacted] à la Cnam) • Pour le fichier de suivi / reporting = compétence du Chef de projet DAJ-LCF [redacted]
Hébergement des données	Cnam [redacted]
Intégration des données	Shift Technology (accès des données au personnel autorisé et habilité en conséquence)
Conception de scénarii d'aide à la détection de fraudes et autres	Shift Technology (personnel autorisé et habilité en conséquence)
Exploitation des données et scénarii	Les agents du département lutte contre la fraude (plus particulièrement ceux du pôle détection et investigation) et de la mission paiement à bon droit (DCF) auront accès aux données au travers de l'interface utilisateur Shift afin de réaliser les contrôles « fraudes » proposés par la solution proposée par Shift. • Exploitation des alertes pour les agents de la LCF • Exploitation des doublons pour les agents de la MPBD
Conservation et suppression des données	- Pour la Cpam : Conservation actée pour 3 ans conformément à la réglementation en vigueur (décret n°2015-389 du 3/04/2015) - Pour la Cnam : conservation actée jusqu'au terme de l'expérimentation - Pour Shift : aucune conservation, ni copie des données. Suppression prévue à la fin de l'expérimentation , mais également à tout moment sur demande des autres cocontractants
Reporting	Cheffe de projet Shift + Chef de projet LCF Cpam de Paris

Autres fonctions	- **Respect de l'intégrité et confidentialité des données** : en cas de violation des données à caractère personnel, la procédure de notification telle qu'inscrite dans la convention devra être appliquée. Ladite notification devra être transmise aux DPO de la Cnam et de la Cpam de Paris. Le sous-traitant est chargé de prendre les mesures indispensables pour remédier à la violation pour, notamment, en limiter les conséquences les plus fâcheuses. - **Transfert des données par le sous-traitant** : ce dernier n'est pas prévu et est formellement interdit en dehors de l'espace économique européen (cf. supra)

	Qui fait *(préciser profil métier, service ou organisme)*
Saisie	Oui Agents du PDI et la MPBD [redacted]
Consultation	Oui DAJ-LCF [redacted] MPBD PESI [redacted] DSI [redacted]
Import	Oui DAJ-LCF [redacted]
Export	Non
Transfert	Non
Edition	Oui DAJ-LCF [redacted] MPBD [redacted]
Reporting	Oui DAJ-LCF [redacted]
Modification	DAJ-LCF [redacted]

	MPBD [redacted]
Mise à jour	Oui par Shift uniquement
Validation	Non
Suppression	Oui mais uniquement des commentaires inscrits par les agents disposant du profil "technicien" DAJ-LCF [redacted] MPBD
Autres fonctions	Non

Administration	
Qu'est-ce qui est administrable	***Par qui (préciser les profils, services ou organismes)***
Assignation alertes	DAJ-LCF [redacted]
Création des utilisateurs dans des groupes	DAJ-LCF
Verrouillage / déverrouillage des utilisateurs	DAJ-LCF

Concernant l'utilisation des données, indiquez

	Réponses
Origine des données *(base de données et laquelle ; saisie, récupération …)*	Requête [redacted] reprenant l'ensemble des facturations audio / optique [redacted]
Durées de conservation des données, indiquez ce qui justifie la durée (traitement courant, archives intermédiaires, autre : préciser)	La Cpam de Paris ne conserve pas les fichiers de données déposés ou générés sur le serveur de la Cnam plus que nécessaire : ⇨ Les données enregistrées dans les outils de gestion des alertes sont conservées pour une durée maximale de **5 ans**. Toute alerte non pertinente est supprimée sans délai. ⇨ Les données de signalement des fautes, abus et fraudes et anomalies sont conservées pour des durées maximales de : ▪ **1 an** pour les dossiers classés sans suite par l'organisme ou ayant fait l'objet d'une décision de non-lieu ou de relaxe à compter de la date de cette décision ;

	Réponses
	▪ **1 an** pour les dossiers classés sans suite par le procureur de la République, sauf s'ils font encore l'objet d'une procédure de sanction ou conventionnelle ; ▪ **5 ans** à compter de l'intervention d'une décision définitive en cas de contentieux, dans les autres cas. ⇨ Les données issues de requêtes pour la réalisation du ciblage des dossiers à contrôler sont conservées jusqu'au ciblage suivant sur le même type de faute, abus ou fraude ou la même personne et pendant une durée qui ne peut excéder **3 ans**. Ces durées sont celles qui avaient fait l'objet d'une demande d'avis à la Cnil sur le projet de décret en conseil d'Etat de 2015 *(Décret n°2015-389 du 3 avril 2015 autorisant les traitements automatisés de données à caractère personnel et les échanges d'informations mis en œuvre par les organismes gestionnaires des régimes obligatoires de base de l'Assurance Maladie pour l'accomplissement de leurs missions en matière de lutte contre les fautes, abus et fraudes.* La Cnam ne conserve pas les fichiers de données déposés ou générés sur le serveur de la CNAM plus que nécessaire à leur traitement. Le fichier et les données seront détruits, ainsi que leurs copies, à la fin de l'expérimentation de la solution SHIFT. Enfin, SHIFT Technology ne conserve aucune donnée, et ne réalise aucune copie de données contenue au sein de sa solution hébergée par la Cnam en dehors de l'infrastructure hébergée par la CNAM. En cas de stockage de données personnelles complémentaires, SHIFT s'engage à détruire l'ensemble des données et les copies dès la fin de l'expérimentation ou sur ordre écrit des responsables du traitement.
Destruction automatique des données à prévoir ?	**Oui** : ⇨ La Cnam s'engage à détruire l'ensemble des données, ainsi que leurs copies, dès la fin de l'expérimentation ; ⇨ SHIFT Technology s'engage également à détruire l'ensemble des données et les copies dès la fin de l'expérimentation mais aussi sur ordre écrit des responsables du traitement.

	Réponses
Archivage des données à prévoir ?	**Oui** [redacted]
Si oui, **durée d'archivage**	**Oui :** au-delà de leur délai de conservation, les données mentionnées (à l'exception des données relatives aux dossiers classés sans suite) peuvent être archivées pour une période de **5 ans maximum** dans un environnement logique séparé, aux fins d'évaluation.
Si oui, **nature des données à archiver** (données nominatives et lesquelles ? ou données anonymes à des fins de statistiques, ...)	Données issues de la requête [redacted] reprenant l'ensemble des facturations audio / optique à examiner par Shift *cf. supra tableau figurant au point 2.1*
Les **destinataires** (au sens communication des données) : - *En interne* - *En externe*	***En interne*** : Département de la Lutte contre de la Fraude, mission paiement à bon droit de la Direction comptable et financière, PESI et DSI
	En externe : SHIFT Technology
Lieu de stockage des données	Le Produit SaaS est hébergé dans les infrastructures de la **CNAM** [redacted] selon les prérequis techniques convenus entre les 3 signataires de la convention. La société Shift n'a pas la possibilité et s'interdit même de transférer la moindre de ces données en dehors de l'espace économique européen, à défaut d'instructions expresses du responsable du traitement et en s'engageant expressément à satisfaire les exigences spécifiques du droit de l'Union ou du droit de l'Etat membre à laquelle les parties sont soumises et conformément au RGPD.
Utilisation d'objets connectés ou smartphone ou tablettes (si mise à disposition des utilisateurs des objets connectés ou smartphones ou tablettes)	Non

2.2 Mesures relatives à la sous-traitance et aux mutualisations

	Réponses
Fait-on appel à un **sous-traitant ou à un organisme extérieur** (ex : autre organisme dans le cadre de TRAM, CTI, ...).	**Oui :** le prestataire SHIFT Technology, disposant de la qualité de sous-traitant dans la convention tripartite d'expérimentation (*au sens de l'article 4, 8° du RGPD*).
Les **obligations des sous-traitants** sont-elles clairement définies et contractualisées (ex : convention) ? **NB** : *Pour TRAM, juridiquement l'organisme prenant est bel et bien un sous-traitant (au sens de la loi Informatique et Libertés). Néanmoins, afin de limiter la complexité de gestion pour les DPO nous n'allons pas faire de registre pour la sous-traitance. Par contre il apparait nécessaire d'avoir une convention*	**Oui :** la convention d'expérimentation tripartite "SHIFT" signée le 18/03/2025 définit dans son article 4.1 les obligations incombant au sous-traitant SHIFT Technology vis-à-vis des responsables du traitement. [redacted]

2.3 Mesures relatives aux accès à l'application

	Réponses
L'applicatif sera-t-il **sécurisé par des habilitations PASSEPORT (Access Master)** ? ***Si non***, décrire le mécanisme d'authentification et d'identification ?	*[PHASE 1 avant expérimetation] Non. Chaque intervenant de Shift Technology, de la CPAM de Paris et de la CNAM est authentifié par un identifiant unique en combinaison avec des moyens d'authentification forte multi-facteur.* *Les mots de passe des utilisateurs ne sont pas stockés en clair dans le système d'information. La règle par défaut pour les périmètres est d'utiliser des fonctions de chiffrement non réversibles de type « hashage » avec des algorithmes sécurisés* *[PHASE 2 au démarrage de l'expérimentation] Non. Accès à l'interface utilisateur par identifiant (adresse professionnelle de chaque agent) + mot de passe (créé et administré par Shift, et transmis de façon asynchrone individuellement à chaque agent par mail).*
Existe-t-il une **stricte séparation entre ordonnateur et contrôle** ?	Non applicable
Définir et détailler les profils applicatifs (ex services Access Master), les **profils métiers** dans lesquels intégrer ces profils applicatifs et le **périmètre des habilitations**	3 profils administrés par Shift : [redacted]
Convient-il de **créer ou modifier les délégations**? Si oui, préciser	Non

2.4 Mesures relatives aux échanges de données

	Réponses
Les données sortent-elles de l'organisme ? (O/N) si oui lesquelles ?	**Oui :** - données décrites dans le paragraphe 2.1 (informations relatives aux données) - tableau de suivi / reporting (clef en commun avec Shift)
Transmission à un autre organisme du réseau de l'Assurance Maladie, transmission hors du réseau de l'Assurance Maladie ? …	**Oui :** - le service informatique de la CPAM de Paris transmet à la Cnam les fichiers de données pseudonymisées par ses soins (via un outil dédié de la CPAM) [redacted] - le chef de projet LCF transmet par envoi sécurisé à Shift le Tableau de suivi / reporting Shift [redacted]
Préciser par quel moyen *(mail, dépôt sur un serveur PETRA, courrier, transfert sécurisé, etc…)*	- Dépôt des fichiers de données pseudonymisées via un applicatif sécurisé [redacted] - Transmission du tableau de suivi / reporting Shift via un applicatif sécurisé [redacted]
En cas de transmission, doit-on s'assurer de la bonne réception sans modification ?	**Oui :** - Dépôt des fichiers de données pseudonymisées = accusé de réception [redacted] - Transmission du tableau de suivi / reporting Shift = accusé de réception [redacted]

2.5 Mesures relatives aux cas de panne ou accès impossible

	Réponses
Quels sont les **créneaux de disponibilité demandés pour cette application** ? (24/24, jours ouvrés, heures ouvrées, ...)	[redacted]
Quelle est la **durée maximale d'interruption acceptable**? Exprimée en heure, ou en jour, ou en semaine ...	[redacted]
Quel sont les **impacts en cas d'indisponibilité** ?	Pas de traitement des signalements
Perte de données maximale acceptable (en jours) - (induit des mécanismes de sauvegarde appropriés)	NC
En cas d'indisponibilité supérieure à la durée maximale d'interruption acceptable, faut-il définir un **moyen de contournement** ? Propositions éventuelles	Traitement des signalements en mode local.

2.6 Modifications non désirées, disparition, vol ou accès illégitime à des données

	Réponses
Des informations sont-elles **potentiellement présentes sur un support transportable** (clé USB, DVD, ordinateur portable,…) ?	[redacted]
Quelles pourraient en être les **conséquences** (aucune, gênantes mais sans impact sur l'activité, grave avec interruption de l'activité,..)?	[redacted]
Quelles sources pourraient-elles en être **à l'origine** *(ex : personne non habilitée ayant accès à l'application, vol de support amovible, erreur humaine, …)* ?	[redacted]
Quelles sont les **principales menaces** *(fraude interne, virus, récupération d'un identifiant mot de passe, utilisation d'une carte agent, accès motivé par la curiosité et non par une justification professionnelle, …)* qui pourraient permettre la réalisation du risque ?	[redacted]
Quels pourraient être les **principaux impacts** si le risque se produisait *(impact financier, image, dépôt de plainte, …)*?	[redacted]

2.7 Traces de connexions et traces applicatives

	Réponses
Convient-il de **conserver les traces de connexions** ?	[redacted]
De quelles **opérations** ou **informations** doit-on **conserver des traces** ? (Traces de connexion, traces sur les opérations (lecture ou mise à jour)	[redacted]
Quelle est la **durée de conservation des traces** ?	[redacted]

2.8 Mesures demandées ou souhaitées par le demandeur métier (MOA)

Possibilité d'intégrer dans ce paragraphe toutes les informations correspondant à des questions non posées précédemment.

Ex : Protection particulière physique ou logique du poste de travail.

	Réponses
Accès à l'outil Shift pour les agents en télétravail	Accord de la CNAM et transmission des ID VPN de chaque agent habilité

2.9 Mesures existantes ou prévues par la MOE

	Réponses
Est-ce que les données sont **hébergées hors Union européenne** ? En cas de transfert de données en dehors de l'Union européenne, si oui précisez ?	Non : les données sont hébergées par la Cnam, sur des serveurs dédiés [redacted] Comme vu *supra* : la société Shift n'a pas la possibilité et s'interdit de transférer les données en dehors de l'espace économique européen, à défaut d'instructions expresses du responsable du traitement et en s'engageant expressément à satisfaire les exigences spécifiques du droit de l'Union ou du droit de l'Etat membre à laquelle les parties sont soumises et conformément au RGPD.
Est-ce que des **données de santé font partie des données hébergées en interne et/ou en externe** ? si oui précisez les mesures de sécurisation	Oui, données récupérées et pseudonymisées par la Cpam de Paris avant adressage [redacted]
Quels sont les **documents préalables** à la mise en production ?	Signature de la convention tripartite Contrat Documentation
Un **PV** (Procès-Verbal) **de recette**, **CBF** (Constat de Bon Fonctionnement), ou **VSR** (Vérification de Service Régulier) sont-ils indispensables ?	Oui [redacted]
Les **traces** sont-elles **externalisées** ? Si oui, préciser *(sur un autre serveur que celui des données)*	[redacted]
Préciser les mesures que la MOE prévoit de mettre en œuvre au regard des risques.	Pseudonymisation des données sensibles (par un outil dédié de la CPAM) [redacted]
Utilisation **d'objets amovibles, d'objets connectés ou smartphone ou tablettes** ? si oui préciser la sécurisation associée.	Non

2.10 Questionnement DPO

	Réponses
Information préalable des personnes concernées Comment les personnes concernées sont-elles informées à propos du traitement *? (Mention d'information sur un formulaire de recueil des données (papier, internet…), Mention d'information sur site Internet, Oralement, Envoi d'un courrier personnalisé, Affichage, Autre, préciser)* Fournir les mentions pour relecture et préciser leur origine ***NB*** : Vérifier la nécessité d'informer les IRP	Conformément aux articles 5, 12, 13 ou 14 du RGPD relatifs à la transparence sur les traitements et sur les informations à communiquer aux personnes concernées, les informations figurent dans la politique générale de protection des données personnelles présente sur ameli.fr En plus de cette information générale, une information individuelle est apportée aux personnes concernées pour qu'elles soient en mesure de pouvoir apporter des observations dans le respect du contradictoire. L'information est fournie par courriers aux personnes concernées selon des modalités qui diffèrent selon l'issue des investigations. [redacted] Mention d'information à intégrer dans les courriers d'information des constats réalisés ouvrant la période de contradictoire : « Vos données personnelles sont traitées par la CPAM de Paris dans le cadre de son obligation légale de contrôle des prestations en matière de lutte contre les fraudes des professionnels de santé en application de l'article L.114-9 du code de la sécurité sociale. Les données analysées sont celles contenues dans les ordonnances et facturations de soins ou produits que vous avez dispensés et sont conservées trois ans. La présente décision a été prise sur le fondement d'un traitement algorithmique d'aide à la détection d'incohérences ou d'anomalies. La vérification et la validation de la décision sont toujours réalisées par un agent de la CPAM de Paris. Vous disposez de droits d'accès et de rectification que vous pouvez exercer auprès du directeur de votre Caisse ou de son délégué à la protection des données (dpo.cpam-paris@assurance-maladie.fr ou **21, rue Georges Auric 75948 Paris cedex 19).** Si vous estimez, après nous avoir contactés, que vos droits « Informatique et Libertés » ne sont pas respectés, vous pouvez adresser une réclamation à la Commission nationale de l'informatique et des libertés (CNIL) **3, place de Fontenoy – TSA - 80715 – 75334** Vous disposez également d'un droit de communication des règles définissant ce traitement algorithmique réalisé par la CPAM de Paris et des principales caractéristiques de sa mise en œuvre. En l'absence de réponse dans un délai d'un mois suivant la réception de votre demande de communication par nos services, vous pouvez saisir pour avis, dans un délai de deux mois à compter de la notification du refus ou de l'intervention du refus tacite, la commission d'accès aux documents administratifs **(CADA – TSA 50730 - 75334 PARIS CEDEX 07).** » [redacted]

	Réponses
	[redacted] Présentation en séance plénière du Comité Social et Economique du le 10/07/2025, avec avis rendu le jour même
Si applicable, comment le consentement des personnes concernées est-il obtenu ?	NC
Comment le consentement peut-il être retiré ?	NC
Si traitement avec « opt out » : comment la personne peut-elle exprimer sa volonté de sortir (ex : newsletter) ? Opt out = moyen de désinscription d'un abonnement	NC
Le droit d'opposition s'applique-t-il au traitement de données ?	Non : il s'agit d'une obligation d'ordre légal.
Comment les personnes concernées peuvent-elles exercer leurs droits d'accès, de rectification, d'opposition ...?	Les droits d'accès et de rectification s'exercent auprès du directeur de la caisse de rattachement de la personne concernée en contactant le DPO.
Le traitement de données entre-t-il dans le champ : ○ d'une publication de la CNIL ▪ *ligne directrice* ▪ *référentiel ou une recommandation* ▪ *méthodologie de référence* ▪ *règlement type* ○ d'un code de conduite sectoriel	NC
Le projet prend-t-il en compte le principe de minimisation des données, c'est-à-dire les données strictement nécessaires au traitement ?	Oui

2.11 Questionnement MSSI

	Réponses
Mesures relatives aux accès à l'application Des antinomies ou conflits d'habilitations sont-elles possibles? Si oui, préciser lesquelles	[redacted]
Modifications non désirées, disparitions ou vols de données Quelle est la probabilité que le risque survienne ? *(1, 2, 3, 4 :* ○ *1 : très peu probable (notion de long terme, soit + de 10 ans)* ○ *2 : peu probable (notion de moyen terme = quelques années)* ○ *3 : moyennement probable (notion de court terme, soit environ 12 mois)* ○ *4 : prochain (dans l'année))* **Justifier le choix**	[redacted]
Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ? Comment estimez-vous la gravité du risque résiduel *(négligeable, faible, forte, très forte ?)*?	[redacted]

	Réponses
Accès illégitime à des données Comment estimez-vous la gravité du risque (négligeable, faible, forte ?), notamment en fonction des impacts potentiels et des mesures prévues ? Quelle est la probabilité que le risque survienne, notamment au regard des menaces, des sources de risques et des mesures prévues ?	[redacted]
Le **besoin de disponibilité de l'outil** est-il couvert par des solutions ?	[redacted]

2.12 Avis

2.12.1 Avis du MSSI et du DPO

Avis du MSSI	*Avis du DPO*
☑ Avis favorable ☐ Avis favorable avec réserves (préciser les réserves dans la partie « mesures nécessaires ») ☐ L'analyse nécessite une étude plus approfondie ☐ Avis défavorable et motif : ☐ Mesures nécessaires pour traiter les risques résiduels :	☑ Avis favorable ☐ Accepté sous condition d'améliorations - Mesures d'amélioration : ☐ Non accepté - à corriger - Mesures correctrices **Actions *à engager* par le DPO :** ☒ Inscription au registre ☐ Mention d'information ☐ Autres formalités (demande d'autorisation, ….

Risques résiduels				
Critère de sécurité (DICP)	*Exposé des risques*	*Objectifs de sécurité*	*Solutions de sécurité / Dispositifs de protection*	*Qualification risques (mineur/limité, important/gênant, majeur)*
Disponibilité	-	-	-	-
intégrité	-	-	-	-
Confidentialité	-	-	-	-
Preuves	-	-	-	-

Commentaires du MSSI	*Commentaires du DPO*
Signature du MSSI	***Signature DPO***
Prénom/nom : [redacted] Date : 20/08/2025 Signature : [redacted]	Prénom/nom : [redacted] Date : 20/08/2025 Signature : [redacted]

☑ *Information nécessaire aux IRP (alerte au responsable de traitement)*

☐ **Arbitrage Direction**

2.12.2 Validation de la Direction

Validation du Directeur Comptable et Financier	Validation du Directeur de l'organisme
Prénom/nom : [redacted] Date : 20 08 2025 Signature : [redacted]	*Prénom/nom* [redacted] Date : 27 08 2025 Signature : [redacted]