

Convention de droit d'usage des données PMSI

ENTRE LES PARTIES :

Le Responsable de la mise en œuvre du traitement :

Nom :

adresse :

Représenté par son "titre du représentant" :

Nom du représentant :

Premièrement,

L'Agence technique de l'information sur l'hospitalisation (ATIH)

Deuxièmement,

Visas :

- Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;
- Vu le code de la santé publique, notamment ses articles L. 1460-1 à L. 1461-7 ;
- Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 34 et 35 ;
- Vu la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé;
- Vu le décret n° 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national de données de santé »;
- Vu l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé;
- Vu l'engagement de conformité prévu pour les laboratoires de recherche et les bureaux d'études conformément à l'arrêté du 17 juillet 2017 relatif au référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études;

Les Parties s'étant rapprochées ont convenu de ce qui suit :

PRÉAMBULE

La présente convention est conclue dans le cadre de la mise en œuvre de traitements mobilisant des données du PMSI, à des fins de recherche, d'étude ou d'évaluation au sens du 1° du I de l'article L. 1461-3 du code de la santé publique, pour lequel l'ATIH est Responsable de traitement.

La loi de modernisation de notre système de santé de 2016 a réformé les conditions d'accès aux données de santé.

Conformément au 3° du IV du L. 1461-1 du code de la santé publique, l'accès aux données s'effectue dans des conditions assurant la confidentialité et l'intégrité des données et la traçabilité des accès et des autres traitements, en conformité avec le référentiel de sécurité défini par arrêté du 22 mars 2017 précité.

L'article L. 1461-1-V du code de santé publique dispose que les finalités de traitement suivantes sont interdites :

- La promotion des produits mentionnés au II de l'article L. 5311-1 en direction des professionnels de santé ou d'établissements de santé ;
- L'exclusion de garanties des contrats d'assurance et la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

Les personnes commercialisant des produits de santé et les personnes exerçant une activité d'assurance ne peuvent accéder aux données du PMSI qu'en :

- démontrant que les modalités de mise en œuvre des traitements rendent impossible toute utilisation des données pour l'une des finalités interdites ;
- en ayant recours à un laboratoire de recherche ou un bureau d'études.

L'arrêté du 17 juillet 2017 relatif au référentiel déterminant les critères de confidentialité, d'expertise et d'indépendance pour les laboratoires de recherche et bureaux d'études précise les critères auxquels ces structures doivent se déclarer conformes pour assurer la mise en œuvre de traitements de données du SNDS commandités par des personnes commercialisant des produits de santé et les personnes exerçant une activité d'assurance.

Une méthodologie de référence (MR006) permet d'encadrer la plupart des projets des industriels dans le domaine des médicaments et des dispositifs médicaux afin de les dispenser d'une procédure d'autorisation au cas par cas. La contrepartie de cet allègement des formalités est une plus grande transparence sur les traitements menés et leur enregistrement dans un répertoire public tenu par l'Institut national des données de santé (INDS).

Pour les autres traitements, le Responsable de traitement ou le Responsable de la mise en œuvre, pour le compte de ce dernier, doit renseigner un dossier auprès de l'INDS pour solliciter une autorisation de la Commission Nationale de l'Informatique et des Libertés (CNIL) après avis du comité d'expertise pour les recherches, les études et les évaluations (CEREES).

Les personnes responsables des traitements sur les données du PMSI ainsi que celles les mettant en œuvre ou autorisées à y accéder sont soumises au secret professionnel dans les conditions et sous les peines prévues à l'article L. 226-13 du code pénal.

ARTICLE 1 - OBJET DE LA CONVENTION

La présente convention a pour objet de rappeler les droits et les obligations de chacune des Parties, de déterminer les modalités de mise à disposition des données du PMSI au Responsable de la mise en œuvre des traitements, les modalités d'utilisation de ces données par ce dernier et les modalités de facturation de l'accès à ces données.

L'ATIH transmettra toute nouvelle base au Responsable de la mise en œuvre du traitement uniquement s'il en a fait la demande et s'il a été au préalable déclaré auprès de l'ATIH comme agissant en tant que Responsable de la mise en œuvre d'un traitement de ces données par un responsable de traitement

ARTICLE 2 - DOCUMENTS CONVENTIONNELS

Les Parties s'engagent sur les documents suivants :

- La présente convention ;
- Annexes
 - l'expression des besoins en données du PMSI pour les traitements objets de la présente convention, présentée en annexe 1,
 - la liste des Utilisateurs, et notamment celle du référent à qui seront adressées les données, qui pourront accéder aux données nécessaires à la réalisation des traitements objets de la présente convention, (annexe 2)
 - le modèle des conditions générales d'utilisation (CGU) des données du PMSI, (annexe 3),
 - la décision d'homologation de la bulle sécurisée, le compte rendu de la commission d'homologation et l'analyse de risque, (annexe 4)
 - en fin d'année, le recensement de tous les traitements réalisés sur les données du PMSI par Responsable de traitement et par catégorie de traitement, selon le modèle de l'annexe 5.
 - Méthode de génération des clés de cryptage pour le téléchargement des bases du PMSI et méthode de décryptage des bases téléchargées (annexe 6).

ARTICLE 3 - DEFINITIONS

Les « Parties » sont les signataires de la présente convention. Elles sont conjointement désignées par « Parties » et individuellement par « Partie ».

Le « Responsable de traitement » est celui qui définit les finalités du traitement et ses modalités de mise en œuvre. En cas de traitement s'inscrivant dans un circuit classique, c'est lui qui obtient de la CNIL l'autorisation de faire réaliser ce traitement.

Le « Responsable de la mise en œuvre de traitement » est la personne physique ou morale, désignée par le Responsable de traitement, agissant sous sa responsabilité. Responsable du bon déroulement du projet de recherche, d'étude, ou d'évaluation, il a, à ce titre, la charge de la réalisation du(es) traitement(s) et veille à la sécurité des informations de ce(s) traitement(s), ainsi qu'au respect de ses(leurs) finalités. Lorsque le(s) traitement(s) est(sont) commandité(s) par des personnes produisant ou commercialisant des produits mentionnés au II de l'article L. 5311-1 du code de la santé publique ou des organismes mentionnés au 1° du A et aux 1°, 2°, 3°, 5° et 6° du B du I de l'article L. 612-2 du code monétaire et financier ainsi que des intermédiaires d'assurance mentionnés à l'article L. 511-1 du code des assurances, le laboratoire de recherche ou le bureau d'études qui le(s) met en œuvre présente un engagement de conformité conformément aux dispositions de l'arrêté du 17 juillet 2017 précité auprès de la CNIL.

L' « Utilisateur » est la personne physique autorisée à accéder aux données du PMSI pour la réalisation du(es) traitement(s) objet de la présente convention.

Une "Bulle sécurisée" est, selon l'arrêté du 22 mars 2017 précité, un système hébergeant ou mettant à disposition des données relatives au PMSI cédées par l'ATIH.

ARTICLE 4 - ENGAGEMENTS RELATIFS AU TRAITEMENT DES DONNEES

Les données du PMSI sont des données à caractère personnel et confidentiel, dont l'accès doit notamment s'effectuer dans les conditions prévues par l'arrêté du 22 mars 2017 précité.

Les Parties s'engagent à respecter les obligations imposées au titre de la législation sur la protection des données à caractère personnel, celles particulières liées au traitement des données du PMSI et, suivant le cas, le cadre défini par l'autorisation donnée par la CNIL ou par la MR006 pour le(s) traitement(s) objet de la présente convention.

Le Responsable de la mise en œuvre du(es) traitement(s) s'engage à :

- respecter les règles encadrant l'utilisation des données du PMSI et notamment les règles du « référentiel de sécurité » ;
- respecter le secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal ;
- veiller à ce que chaque Utilisateur autorisé à accéder aux données s'abstienne de toute action visant la réidentification directe ou indirecte ;

- veiller à ce que les données ne soient pas traitées par une personne non habilitée ;
- veiller à ce que chaque Utilisateur autorisé à accéder aux données n'exporte pas de données sans s'être assuré que les données ne présentent aucun risque de réidentification ;
- interdire l'accès aux données ou leur traitement par une personne non habilitée ;
- ne pas traiter les données pour une finalité interdite du PMSI et selon les cas, pour une finalité autre que celles autorisées par la CNIL, ou celles entrant dans le cadre de la MR006 pour les traitements objets de la présente convention ;
- mettre en œuvre les moyens matériels de protection des données du PMSI, et mettre en œuvre des actions de sensibilisation à destination des Utilisateurs ;
- gérer les habilitations des Utilisateurs qui traiteront les données conformément aux conditions d'habilitation prévues pour le PMSI, dans la limite des besoins des traitements objet de la présente convention et selon les modalités prévues par la présente convention ;
- vérifier que chaque Utilisateur autorisé à accéder aux données a signé les conditions générales d'utilisation (CGU) du PMSI préalablement à l'accès aux données.

ARTICLE 5 – SOUS TRAITANCE

Si, pour la réalisation de traitements objet de la présente convention, il est fait appel à des sous-traitants, ceux-ci doivent présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité.

En cas de sous-traitance, le Responsable de traitement et le Responsable de la mise en œuvre du(es) traitement(s) sont tenus de garantir que le contrat de sous-traitance comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données au même niveau que leurs propres obligations.

Chaque sous-traitant est tenu de faire respecter les règles de sécurité et de confidentialité des données à toute personne susceptible d'intervenir sur les travaux de collaboration.

ARTICLE 6 - ACCES A UNE BULLE SECURISEE ET HABILITATIONS

La mise en œuvre de l'accès aux données du PMSI se fait au sein d'une bulle sécurisée, homologuée conformément aux dispositions du référentiel de sécurité du SNDS précité.

Seuls les Utilisateurs nommément désignés dans l'annexe 2 et habilités sont autorisés à accéder aux données. La désignation d'un nouvel Utilisateur devra, préalablement à son habilitation, faire l'objet d'une modification cette annexe par voie d'avenant à la présente convention.

Pour pouvoir être habilités, les Utilisateurs doivent, préalablement à l'ouverture des accès, avoir :

- signé les CGU du PMSI dont le modèle est annexé à la présente convention (annexe 3),
- été informés des sanctions en cas de non-respect des conditions d'accès aux données du PMSI.

Le Responsable de la mise en œuvre du(es) traitement(s) conserve un exemplaire des CGU signées par chaque utilisateur et transmet à l'ATIH le bordereau attestant de la signature des CGU par les Utilisateurs prévus à la liste en annexe 2.

En complément, le Responsable de la mise en œuvre du(es) traitement(s) s'engage à signaler le statut des Utilisateurs qui interviennent sur une base juridique différente d'un contrat de travail avec lui. Pour ces Utilisateurs, le Responsable de la mise en œuvre du(es) traitement(s) garantit que les modalités d'intervention de l'Utilisateur sont établies dans un cadre contractuel précis qui permet notamment de garantir l'application des obligations en matière de protection de la sécurité et de la confidentialité des données au même niveau que ses propres obligations. Il s'engage à faire signer un engagement de confidentialité à ces Utilisateurs.

Le Responsable de la mise en œuvre du(es) traitement(s) s'engage à informer l'ATIH dans les meilleurs délais du départ d'un des Utilisateurs habilités dans le cadre de la présente convention.

Le Responsable de la mise en œuvre du(es) traitement(s) est responsable de la gestion des Utilisateurs.

ARTICLE 7 - SECURITE DES ECHANGES, MODALITES ET PREUVE DE LA TRANSMISSION ET DE LA RECEPTION DES DONNEES, RECETTE FONCTIONNELLE

7.1 Sécurité des échanges

Afin d'assurer la sécurité de la transmission des données PMSI de l'ATIH vers le responsable de mise en œuvre du(es) traitement(s), celles-ci seront cryptées par l'ATIH au moyen du logiciel GnuPG.

Le logiciel GnuPG est une version libre du standard openPGP mettant en œuvre un mécanisme de cryptographie asymétrique afin de chiffrer les fichiers échangés entre les parties. Ce mécanisme repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder, garantissant la confidentialité du contenu. Les logiciels mettant en œuvre GnuPG sont nombreux et existent dans le monde du logiciel libre sur tous les systèmes d'exploitation.

Le Responsable de la mise en œuvre du(es) traitement(s) enverra sa clé publique par courriel, après l'avoir générée sur sa plateforme, au correspondant désigné au sein de l'ATIH. L'annexe 6 présente les modalités précises de mise en œuvre.

7.2 Modalité de la transmission des données

Pour la durée de la convention, chaque année, dès leur disponibilité au sein de l'ATIH, les tables de données PMSI nationales annuelles scellées sont cryptées par l'ATIH avec la clé publique envoyée par le Responsable de la mise en œuvre du(es) traitement(s) puis transmises.

Les données cryptées sont transmises via la plateforme sécurisée de l'ATIH, par envoi d'un lien sécurisé (https) et temporaire, à l'adresse électronique du seul référent désigné au sein du Responsable de la mise en œuvre du(es) traitement(s) dans l'annexe 2.

Ce lien permet le téléchargement des données une seule et unique fois, dans les 6 (six) jours suivant la notification de mise à disposition.

7.3 Preuve de la réception des données

Un courriel est envoyé automatiquement au référent ainsi qu'au correspondant projet de l'ATIH, lui notifiant la mise à disposition des données sur la plateforme de téléchargement. Ce mail comporte en pièce jointe la liste des fichiers contenus dans l'archive.

Le téléchargement de l'archive est journalisé, l'adresse IP depuis laquelle l'action aura été effectuée sera conservée.

Le référent du Responsable de la mise en œuvre du(es) traitement(s) doit vérifier qu'il est en mesure de lire les données téléchargées, une fois installées puis décryptées sur sa plateforme, et que celles-ci correspondent bien à celles décrites dans la présente convention.

L'ATIH s'engage à transmettre à nouveau les données, selon la procédure standard décrite, si le référent n'a pas reçu les données convenues, ou s'il n'est pas en mesure de lire le contenu des fichiers téléchargés.

ARTICLE 8 - RECETTE DES DONNEES, CONSTAT DE BON FONCTIONNEMENT ET DE CONFORMITE DES DONNEES

Le référent du Responsable de la mise en œuvre du(es) traitement(s) doit vérifier que la qualité des données mises à disposition par l'ATIH est conforme à ses attentes dans un délai de trois (3) mois à compter de la date de mise à disposition de ces données.

Pendant ce délai de trois (3) mois, l'ATIH s'engage à mettre à disposition des données corrigées et/ou complémentaires.

Aucune livraison corrective ou complémentaire ne pourra être effectuée au-delà de ce délai.

ARTICLE 9 - NON RESPECT DES CONDITIONS D'ACCES AUX DONNEES

Le constat fait du non-respect de l'une des conditions d'accès aux données dans le cadre de la présente convention entraînera la suspension immédiate de l'accès de l'Utilisateur concerné voire de tous les accès ouverts au titre de la présente convention.

Un dispositif d'enregistrement des traces d'accès et de suivi des activités des utilisateurs est mis en œuvre, conformément au référentiel de sécurité. L'utilisateur doit être informé de l'existence de ces traces. Il accepte la mise en œuvre de ce dispositif d'enregistrement par la signature des CGU.

Les traces d'accès et de suivi des activités sont conservées au maximum deux (2) ans.

Les données liées à la création et la gestion des comptes des Utilisateurs sont conservées pour la durée d'existence de leur compte.

Une fois un compte Utilisateur fermé, il est possible de conserver certaines données conformément aux durées de prescription légale applicables et aux seules fins de résoudre tout litige, régler tout problème et faire appliquer la présente convention et les CGU.

Des contrôles pourront être conduits sur les traces d'accès et d'utilisation afin de s'assurer que la présente convention et les CGU sont respectées par l'Utilisateur.

Le Responsable de la mise en œuvre du(es) traitement(s) s'engage à mettre tout en œuvre pour faciliter les contrôles et les audits susceptibles d'être réalisés. Les contrats avec ses éventuels sous-traitants doivent impérativement inclure cette disposition.

L'objet de ces audits et contrôles est de s'assurer du respect de la mise en œuvre de la présente convention et de la conformité de la mise en œuvre des traitements aux normes qui lui sont applicables.

La réalisation des audits et des contrôles peut être annoncée ou non en avance.

ARTICLE 10 - GESTION DES INCIDENTS DE SECURITE

En cas de violation de données à caractère personnel, le Responsable de la mise en œuvre du(es) traitement(s) et le Responsable de traitement devront informer l'ATIH immédiatement après en avoir pris connaissance à l'adresse mail rssi@atih.sante.fr. Cette notification devra être accompagnée de toute documentation utile afin de permettre à l'ATIH, si nécessaire, d'adopter les mesures de sécurisation adaptées.

ARTICLE 11 - DROITS DE PROPRIETE INTELLECTUELLE SUR LA PUBLICATION DES RESULTATS

Le Responsable du traitement et/ou le Responsable de la mise en œuvre de traitement pourront publier et communiquer les résultats de leurs travaux (statistiques, analyses, études réalisées à des fins de gestion du risque maladie ou de santé publique) obtenus à partir des données du PMSI,

Par publication et communication, il faut entendre au sens de la présente convention, le droit pour le Responsable de traitement ou le Responsable de la mise en œuvre du(es) traitement(s) de reproduire, représenter et publier les résultats des travaux sous toutes formes et notamment par publications, journaux, imprimés, dépliants, communications sur tous supports dans des congrès et symposiums qu'il organise ou auquel il participe, ou encore par voies électroniques (Internet, Intranet, CD-Rom, DVD), les supports de publication pouvant soit être distribués gracieusement, soit faire l'objet de ventes, prêts ou locations.

Toute publication, sous quelque forme qu'elle soit, devra mentionner le concours respectif des Parties et les sources utilisées soit le PMSI.

Le Responsable de traitement est le seul propriétaire des résultats issus de l'étude.

ARTICLE 12 – DECLARATION DES TRAITEMENTS

Le Responsable de la mise en œuvre s'engage, chaque année, à déclarer à l'ATIH, l'ensemble des traitements demandés par un ou plusieurs Responsable(s) de traitement. La liste des traitements est présentée par catégorie et par Responsable de traitement en annexe 5 de la présente convention.

ARTICLE 13 - CONDITIONS FINANCIERES

Les conditions financières sont celles disponibles sur le site internet de l'agence au jour de la demande de bases <https://www.atih.sante.fr/acces-aux-donnees-pour-les-prestataires-ou-laboratoires-de-recherche>

ARTICLE 14- GESTION DE LA CONVENTION

14-1 Durée

La présente convention prend effet à compter de la date de sa signature et pour une durée de un (1) an et est tacitement reconductible.

14-2 Résiliation

Si les Parties souhaitent mettre un terme à la présente convention, elles doivent le faire par lettre recommandée avec accusé de réception au plus tôt trois (3) mois avant et au plus tard un (1) mois avant la date d'anniversaire de cette convention.

En cas d'inexécution totale ou partielle ou de mauvaise exécution par l'une des Parties de l'une de ses obligations, la présente convention pourra, de plein droit, être résiliée par la Partie la plus diligente. La résiliation ne pourra cependant intervenir que trente (30) jours après l'envoi d'une mise en demeure adressée, par la Partie la plus diligente, par courrier en recommandé avec accusé de réception ou par acte d'huissier à la Partie défaillante, à moins que, dans ce délai, la Partie défaillante :

- n'ait satisfait à ses obligations
- n'ait apporté la preuve d'un empêchement consécutif à un cas de force majeure, ou,
- n'ait proposé une solution de remplacement la plus proche possible de l'objectif recherché.

Cette solution devra être expressément acceptée par l'autre Partie. L'exercice de cette faculté de résiliation ne dispense pas la Partie concernée de remplir les obligations contractées jusqu'à la date de prise d'effet de la résiliation.

14-3 Force majeure

Aucune des Parties ne pourra engager la responsabilité de l'autre si l'exécution du contrat est retardée ou empêchée en raison d'un cas de force majeure, d'un cas fortuit ou d'une cause extérieure, tels que, notamment : catastrophe naturelle, grèves, conflits sociaux, mauvais fonctionnement ou interruption du réseau électrique ou de télécommunication.

La Partie invoquant un événement constitutif de force majeure devra en aviser l'autre Partie dans les sept (7) jours francs suivant la survenance de cet événement.

L'exécution de la convention est suspendue, totalement ou partiellement, pendant le temps où la ou les Parties empêchées se trouvent dans l'impossibilité d'exécuter leurs obligations en raison de la force majeure. Les obligations de la ou les Parties empêchée(s) reprendront dès que l'effet d'empêchement dû à la force majeure cessera, pour la durée restant à courir à la date de survenance dudit cas de force majeure.

Les Parties pourront convenir lorsque la force majeure empêche l'exécution de la convention au-delà de trois (3) mois que :

- la convention est modifiée pour l'adapter aux circonstances nées de la force majeure ou que
- il est mis un terme anticipé à la convention.

14-4 Modifications du contrat

Toute modification de la présente convention ou de ses annexes ne pourra être prise en compte qu'après la signature d'un avenant écrit et signé par le représentant, dûment qualifié, de chacune des parties.

14-5 Renonciation

Sauf dispositions contraires spécifiées dans cette convention, le fait que l'une des Parties n'ait pas exigé l'application d'une clause quelconque de la présente convention ne pourra en aucun cas être considéré comme une renonciation aux droits de cette Partie découlant de ladite clause.

14-6 Règlement des litiges

Pour toute contestation qui s'élèverait entre les Parties, relative à l'interprétation ou à l'exécution de la présente convention, celles-ci s'engagent à soumettre leur différend, préalablement à toute instance judiciaire, à des conciliateurs désignés par chacune d'elles, à moins qu'elles ne s'entendent sur la désignation d'un conciliateur unique. La désignation devra intervenir dans un délai de trente (30) jours à compter de la notification de la contestation à l'autre Partie. Le ou les conciliateurs s'efforceront de régler leurs difficultés et de faire accepter par les Parties une solution amiable dans un délai de soixante (60) jours à compter de la date de désignation du ou des conciliateurs. A défaut de conciliation, la contestation sera portée devant le tribunal administratif compétent.

Fait à Lyon, en deux exemplaires originaux, le

"Le représentant du Responsable de la
mise en oeuvre du(es) traitement(s)"

Le Directeur général de l'ATIH

« Nom du représentant »

Monsieur Housseyni Holla

ANNEXE 1 **Bordereau de commande de base**

**DEMANDE D'ACCES AUX DONNEES ISSUES DES BASES DE RESUMES
D'INFORMATION MEDICALE PMSI ET RIM-P**

DATE DE LA DEMANDE :

Renseignements relatifs au DEMANDEUR

ORGANISME
N° DE SIRET
ADRESSE

NOM / Prénom DU REPRESENTANT LEGAL
FONCTION
E-MAIL@
TELEPHONE
FAX

CONTACT PRINCIPAL <i>(si différent du représentant légal)</i>
<input type="checkbox"/> Madame <input type="checkbox"/> Monsieur
Prénom(s) :
NOM(s) :
Qualité / Fonction :
Tél. :
Nom et adresse de l'unité (si différents de ceux du cadre « organisme ») :
Adresse électronique : email@fournisseur.xx

IDENTITE DE LA PERSONNE POUVANT HABILITER LES UTILISATEURS DE SON ORGANISME
<input type="checkbox"/> Madame <input type="checkbox"/> Monsieur
Prénom(s) :
NOM(s) :
Qualité / Fonction :
Tél. :
Nom et adresse de l'unité (si différents de ceux du cadre « organisme ») :
Adresse électronique : email@fournisseur.xx

Merci de renseigner les informations suivantes relatives aux fichiers du PMSI, ANO et RIM-P faisant l'objet de la présente demande :

		FICHIER(S) ET ANNÉE(S) DEMANDÉS				
	RESUMES ANONYMES	FICHIER DE CHAINAGE ANO (non facturé)	FICHIERS MEDICAMENTS ET DMI DE LA LISTE EN SUS ET MED_ATU			
			ANNEE	MED mco à partir de 2009	MED ATU à partir de 2014	DMI à partir de 2009
MCO	ANNEE(S) :	ANNEE (S) :	A PARTIR DE 2009 ANNEE(S) :		<input type="checkbox"/> ANNEE(S) :	<input type="checkbox"/> ANNEE(S)
			MED_OQN DE 2010 A 2015 : ANNEE (S) : DMI_OQN DE 2010 A 2015 : ANNEE (S) : MED_OQN ET DMI_OQN : DE 2010 A 2015 EXCLUSIVEMENT SECTEUR PRIVE MED ET DMI : AVANT 2016, EXCLUSIVEMENT SECTEUR PUBLIC. A PARTIR DE 2016, SECTEURS PUBLIC + PRIVE RSFA STC* MCO A PARTIR DE 2009 SECTEUR PUBLIC ANNEE (S) : ANO ACE* MCO : non facturé ANNEE (S) :			
SSR	ANNEE(S) :	ANNEE(S) :	Med SSR dès 2011 ANNEE(S) :			
			RSFA DGF SSR* A PARTIR DE 2012 SECTEUR PUBLIC ANNEE (S) : ANO ACE SSR* non facturé <input type="checkbox"/> ANNEE (S) :			
HAD	ANNEE(S) :	ANNEE(S) :	MED HAD dès 2011 ANNEE(S) :			
PSY	ANNEE(S) :	ANNEE(S) :				

- * **RSFA-STC MCO et RSFA DGF SSR** (à partir de 2009 pour le MCO et 2012 pour le SSR) : Résumés Standardisés de Factures Anonymes pour l'activité externe des établissements du secteur public
 * **ANO-ACE** (à partir de 2009 pour le MCO et 2012 pour le SSR) : Fichier de chainage de résumés standardisés de facture anonymes de l'activité externe des établissements du secteur public (ex-DGF)

JE SOUSSIGNE(E),
NOM :
PRENOM :
FONCTION :
CERTIFIE SUR L'HONNEUR L'EXACTITUDE DES RENSEIGNEMENTS FIGURANT DANS LA PRESENTE

A LE
SIGNATURE

LE DEMANDEUR ACCEPTE PAR AVANCE TOUT CONTROLE OPERE PAR L'ATIHI PERMETTANT DE DETERMINER LES CONDITIONS D'UTILISATION DES DONNEES
 TOUTE DECLARATION INSINCERE RENDRAIT CADUQUE LA TRANSMISSION DES BASES ET IRREGULIERE L'UTILISATION QUI EN EST FAITE PAR LE DECLARANT.

Cadre réservé au service

Demande d'investigation complémentaire
 Expertisée par le service Réponse aux demandes externes le/...../.....
 reçue par le pole affaires juridiques le/...../.....

ANNEXE 2

Modèle de liste des personnes habilitées à utiliser les données du PMSI transmises par l'ATIH

Nom	Prénom	Fonction	@ mail	N° de Téléphone	Champ du PMSI (à cocher)			
					MCO	HAD	SSR	Psychiatrie
Référent (1)								

(1) Le lien pour le téléchargement de la base (ou des bases) sera envoyé au mail du référent

ANNEXE 2 (suite)

Modèle de liste des personnes habilitées à utiliser les données du PMSI transmises par l'ATIH

					Champ du PMSI (à cocher)			
Nom	Prénom	Fonction	@ mail	N° de Téléphone	MCO	HAD	SSR	Psychiatrie

ANNEXE 3 Modèle de CGU

Utilisateurs de la plateforme

Peuvent avoir accès à la plateforme les utilisateurs qui sont des personnels du Responsable de la mise en oeuvre du(es) traitement(s) ou liés conventionnellement avec lui, et ayant dans leurs attributions la conduite de travaux de recherche, d'études, de production statistique ou d'outils d'aide à la décision à partir des données composant le PMSI.

Pour obtenir l'accès à la plateforme chaque utilisateur doit prendre connaissance et signer les présentes conditions générales d'utilisation puis transmettre ces documents au référent qui habilite nommément chaque utilisateur pour le traitement concerné. Lorsqu'un utilisateur habilité quitte la structure, il doit en informer le référent et ses droits d'utilisation du serveur sont suspendus.

Les utilisateurs s'engagent à ne pas rapprocher des données individuelles provenant de sources non autorisées avec les données source du PMSI.

Projet de traitement des données par les utilisateurs

Les projets de recherche, d'étude, de production statistique ou d'outils d'aide à la décision, doivent être conformes aux règles s'appliquant au SNDS :

- Ils doivent répondre à une finalité d'intérêt public.
- Ils ne peuvent avoir l'une des finalités suivantes (cf article L.1461-1 du code de santé publique) :
 - la promotion des produits mentionnés au II de l'article L.5311-1 en direction des professionnels de santé ou d'établissements de santé ;
 - l'exclusion de garanties des contrats d'assurance et la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

Accès à la plateforme par les utilisateurs, sécurité

L'accès aux données source du SNDS installées sur la plateforme se fait en lecture seule ; la plateforme n'est pas connectée à l'internet; le traitement des données se fait au moyen de logiciels qui ont été installés sur la plateforme par l'administrateur technique de celle-ci.

Nature des traitements des données par les utilisateurs

Le traitement des données par les utilisateurs doit être conforme aux règles s'appliquant au SNDS :

- Les traitements doivent correspondre au projet de recherche présenté par l'utilisateur et validé; si nécessaire, une modification du projet ou un nouveau projet doit être présenté pour validation au responsable de la plateforme.
- La réidentification des patients, dont les informations figurent dans les données, est interdite.
- L'export hors de la plateforme de données individuelles source ou agrégées non anonymes est interdite.
- Les résultats destinés à être exportés de la plateforme, publiés ou diffusés à des tiers, ne doivent pas permettre la réidentification des personnes considérées et doivent être strictement anonymes ; la source des données doit être mentionnée et des éléments de méthode relatifs au traitement réalisé indiqués.

Conservation des traces informatiques des traitements réalisés par les utilisateurs

L'ensemble des actions et traitements de chaque utilisateur sur la plateforme est enregistré automatiquement dans un espace réservé de celle-ci. Sont également conservées les dates et heures de connexion et déconnexion, les lignes de commandes réalisées, les exports et imports et toute autre opération système...

L'objet de ces traces est de pouvoir contrôler la conformité des actions de chaque utilisateur vis-à-vis des présentes conditions générales d'utilisation et des conditions d'accès aux données du SNDS . Le responsable de la plateforme est le destinataire de ces traces. Chaque utilisateur est identifié nommément dans ces traces, via son authentification. La durée maximale de conservation des traces est de 24 mois. Une déclaration de l'enregistrement de ces traces nominatives a été faite auprès de la Cnil. Conformément à la loi informatique et libertés, chaque utilisateur a accès à ses propres traces ; il exerce ce droit auprès du responsable de la plateforme. Le cas échéant, le responsable de la plateforme sur foi de ces traces et après un entretien contradictoire avec l'utilisateur peut prononcer une suspension de l'accès de l'utilisateur à la plateforme.

Engagement individuel de respect des conditions générales d'utilisation de la plateforme par les utilisateurs

En cas de non-respect par l'utilisateur des règles d'utilisation décrites ci-dessus, l'utilisateur verra son accès à la plateforme suspendu. Cette suspension ne fait pas préjudice aux actions disciplinaires ou judiciaires.

Le signataire reconnaît avoir pris connaissance des présentes conditions générales d'utilisation de la plateforme, dont la traçabilité des actions réalisées sur la plateforme et s'engage à s'y conformer.

Il doit signer deux exemplaires de ce document, en conserver un et transmettre le second à l'administrateur fonctionnel pour transmission au responsable de la plateforme. Son ou ses supérieurs hiérarchiques doivent en être informés.

Nom :

Prénom :

Date :

Signature :

ANNEXE 4

Décision d'homologation de la bulle sécurisée, compte rendu de la commission d'homologation et analyse de risque

ANNEXE 5

Modèle de liste des travaux réalisés par le Responsable de mise en œuvre par Responsable de traitement

Type de demande de traitement (1)	Raison sociale du responsable de traitement	Objet du traitement	Année(s)	Champ(s) du PMSI (à cocher)			
				MCO	HAD	SSR	Psychiatrie

(1) choisir de 1 à 6 dans le menu déroulant pour préciser le cadre de la demande de traitement :

- 1- Méthodologie de référence MR006
- 2- Décision unique (DU)
- 3- Autorisation classique
- 4- Méthodologie de référence MR005
- 5- Accès permanent du Responsable de traitement aux données SNDS
- 6- Autres

ANNEXE 5 (suite) 2/4

Modèle de liste des travaux réalisés par le Responsable de mise en œuvre par Responsable de traitement

Type de demande de traitement (1)	Raison sociale du responsable de traitement	Objet du traitement	Année(s)	Champ(s) du PMSI (à cocher)			
				MCO	HAD	SSR	Psychiatrie

(1) choisir de 1 à 6 dans le menu déroulant pour préciser le cadre de la demande de traitement :

- 1- Méthodologie de référence MR006
- 2- Décision unique (DU)
- 3- Autorisation classique
- 4- Méthodologie de référence MR005
- 5- Accès permanent du Responsable de traitement aux données SNDS
- 6- Autres

ANNEXE 5 suite (3/4)

Modèle de liste des travaux réalisés par le Responsable de mise en œuvre par Responsable de traitement

Type de demande de traitement (1)	Raison sociale du responsable de traitement	Objet du traitement	Année(s)	Champ(s) du PMSI (à cocher)			
				MCO	HAD	SSR	Psychiatrie

(1) choisir de 1 à 6 dans le menu déroulant pour préciser le cadre de la demande de traitement :

- 1- Méthodologie de référence MR006
- 2- Décision unique (DU)
- 3- Autorisation classique
- 4- Méthodologie de référence MR005
- 5- Accès permanent du Responsable de traitement aux données SNDS
- 6- Autres

ANNEXE 5 (suite) (4/4)

Modèle de liste des travaux réalisés par le Responsable de mise en œuvre par Responsable de traitement

Type de demande de traitement (1)	Raison sociale du responsable de traitement	Objet du traitement	Année(s)	Champ(s) du PMSI (à cocher)			
				MCO	HAD	SSR	Psychiatrie

(1) choisir de 1 à 6 dans le menu déroulant pour préciser le cadre de la demande de traitement :

- 1- Méthodologie de référence MR006
- 2- Décision unique (DU)
- 3- Autorisation classique
- 4- Méthodologie de référence MR005
- 5- Accès permanent du Responsable de traitement aux données SNDS
- 6- Autres

ANNEXE 6

Méthode de génération des clés de cryptage pour le téléchargement des bases du PMSI et méthode de décryptage des bases téléchargées

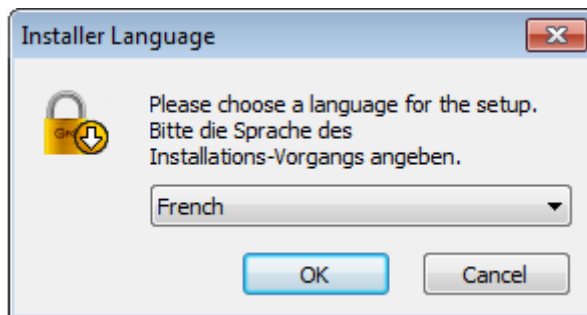
1. Génération d'une clé gpg

Afin de sécuriser l'accès aux bases du PMSI, l'archive contenant les données devra être cryptée par votre clé gpg publique que seule votre clé privée pourra ensuite décrypter.

Afin de générer votre jeu de clés (clé publique+ clé privée), vous devez télécharger le logiciel **gpg4win** depuis cette adresse : <http://www.gpg4win.org/download.html>

1.1 Installation du logiciel

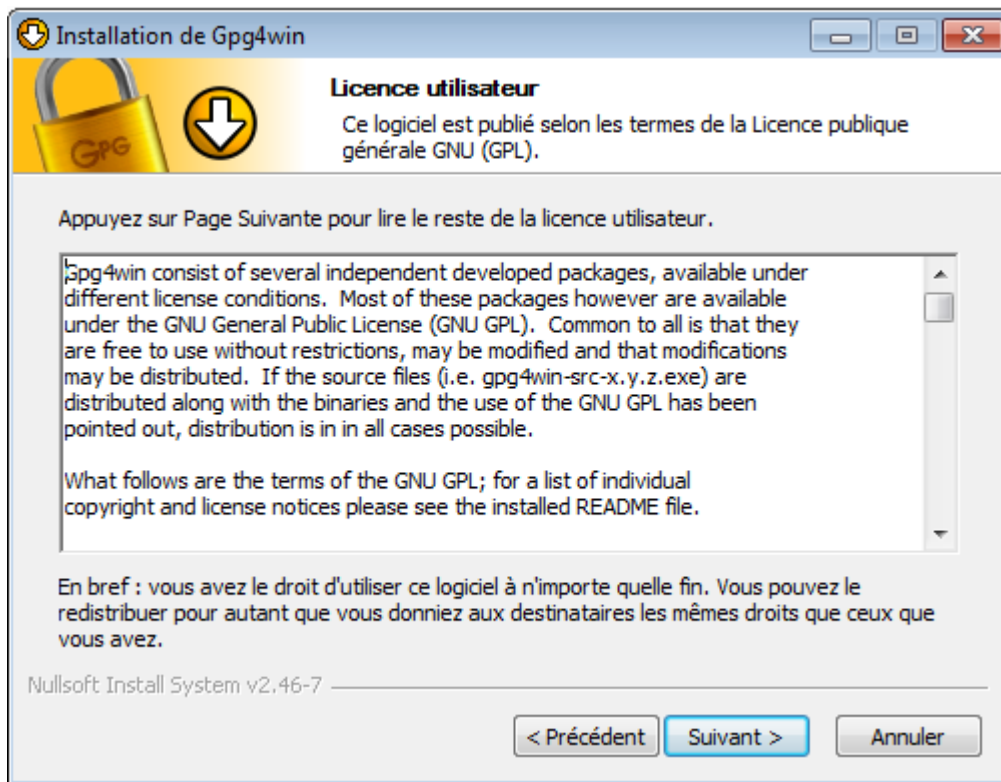
La première étape est la sélection de la langue :



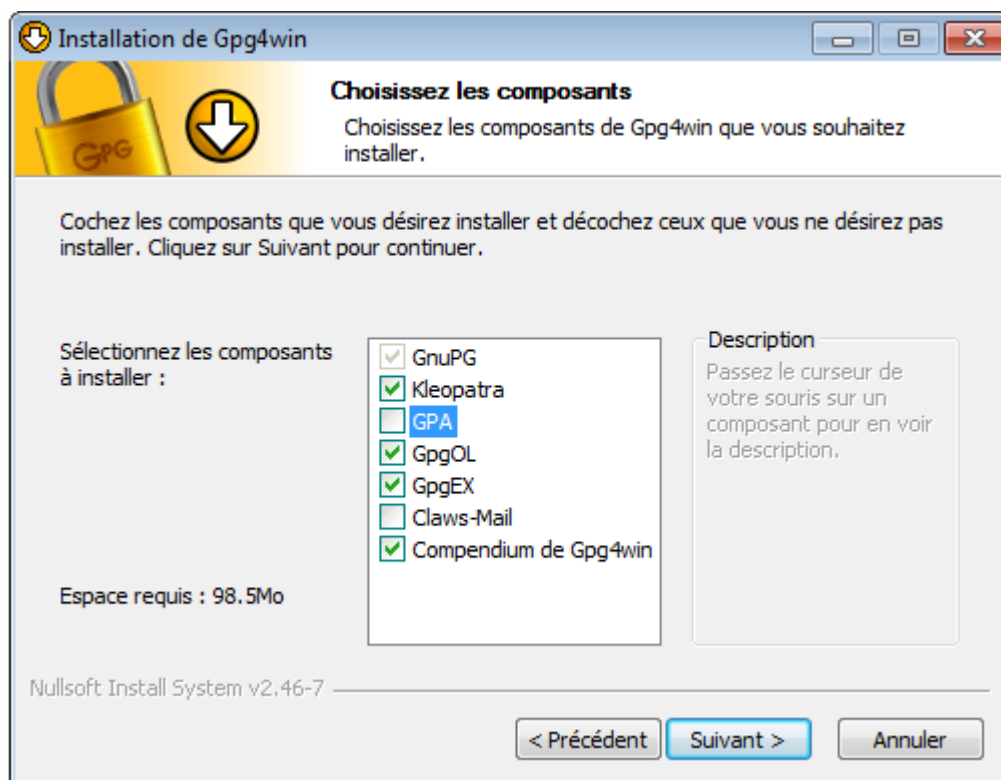
Pour installer le logiciel, cliquer sur *suivant* :



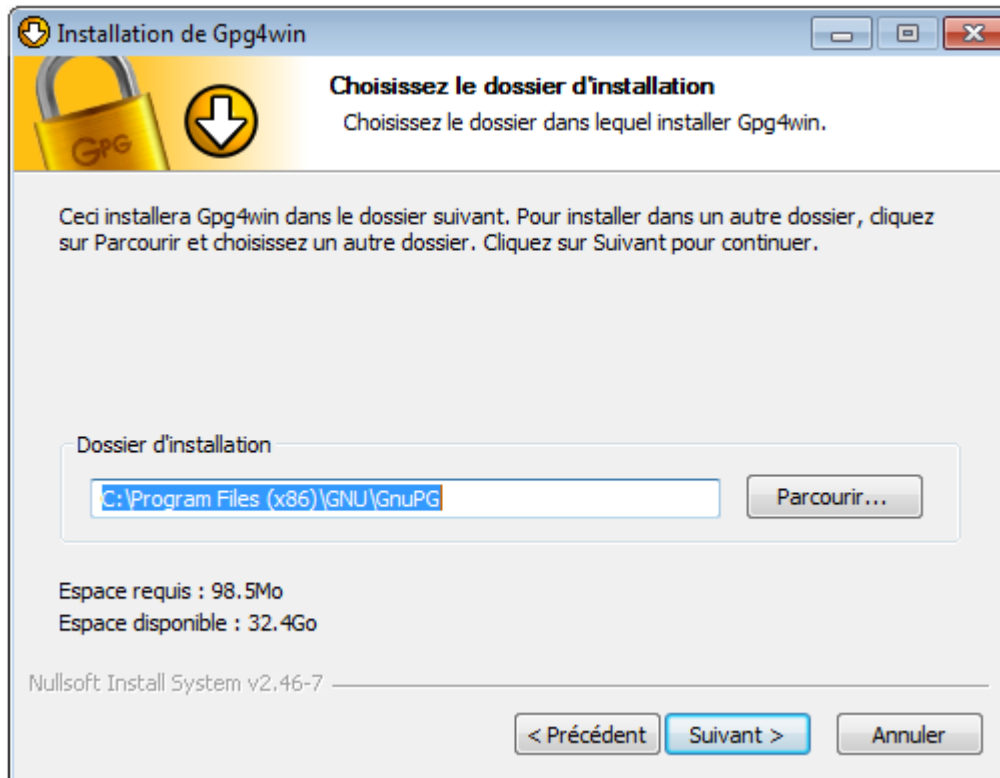
Puis de nouveau sur *suivant* en ayant pris connaissance des termes de la licence :



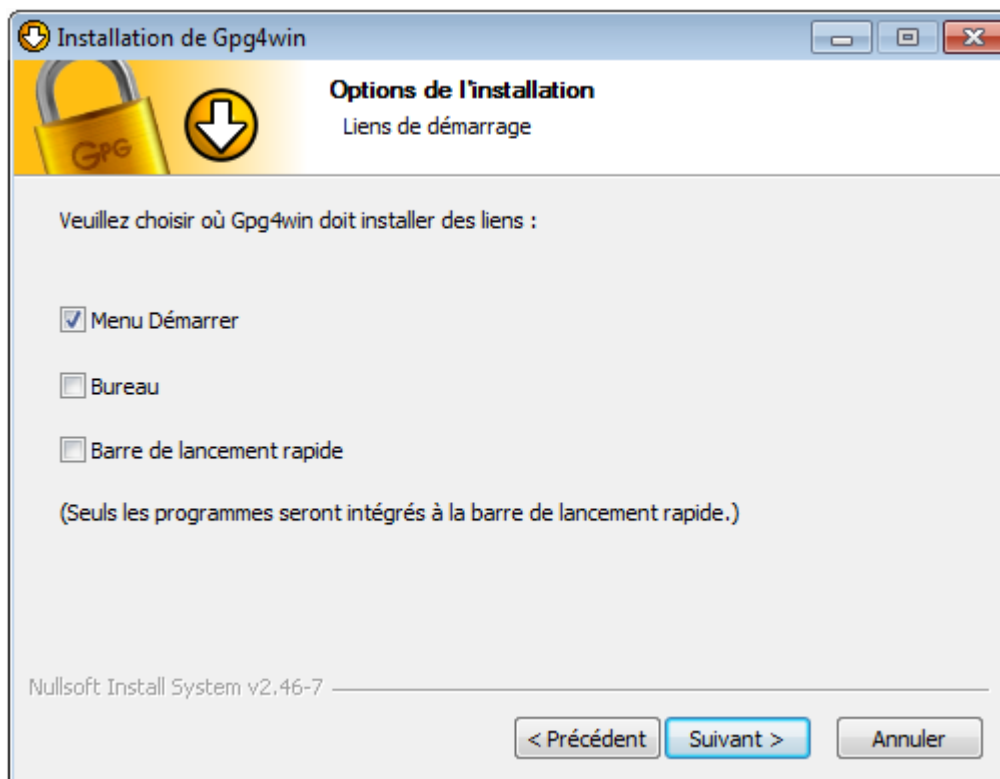
Les composants à installer sont : Kleopatra, GpgOL, GpgEX et Compendium de Gpg4win



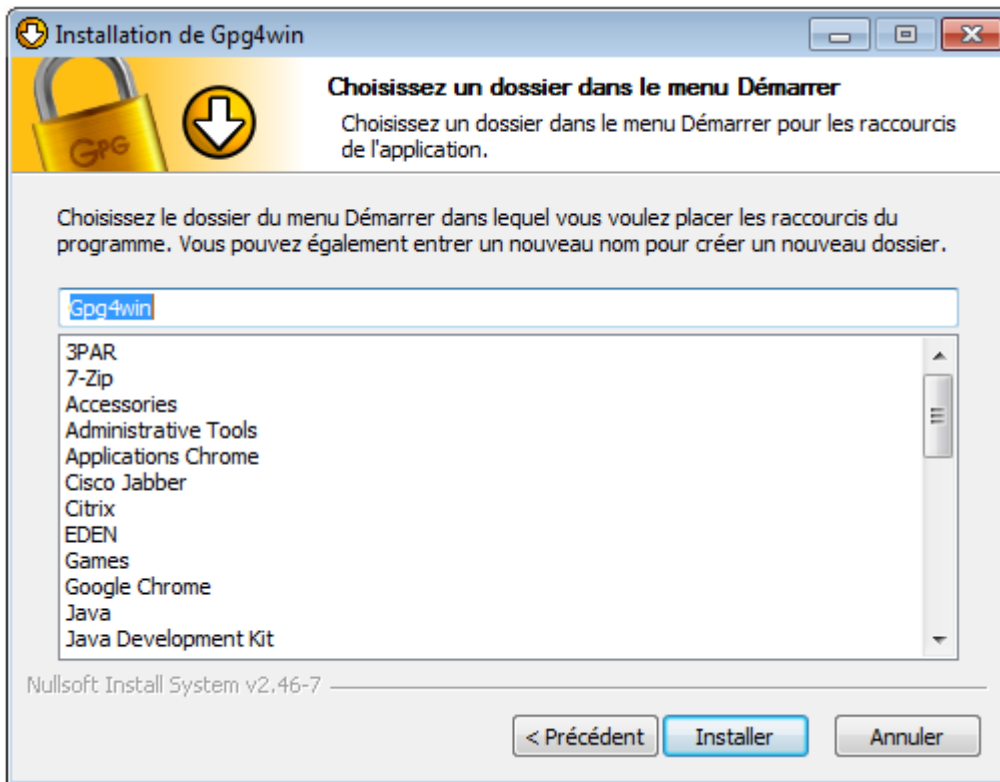
Sélectionner ensuite le répertoire d'installation du logiciel et cliquer sur *suivant*.



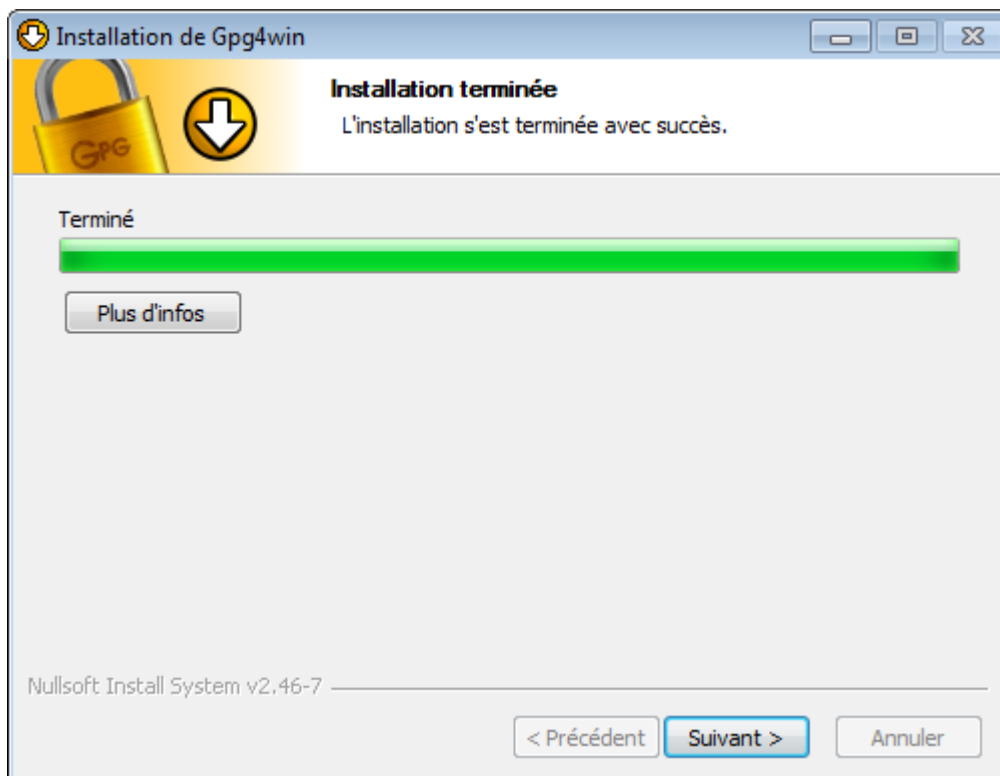
Placer un lien vers le logiciel dans votre menu Démarrer et cliquer sur *suivant* :



Choisissez le nom du dossier qui apparaîtra dans votre menu Démarrer (par défaut :Gpg4win) puis cliquer sur *installer* :



Une fois l'installation terminée, cliquer sur suivant :



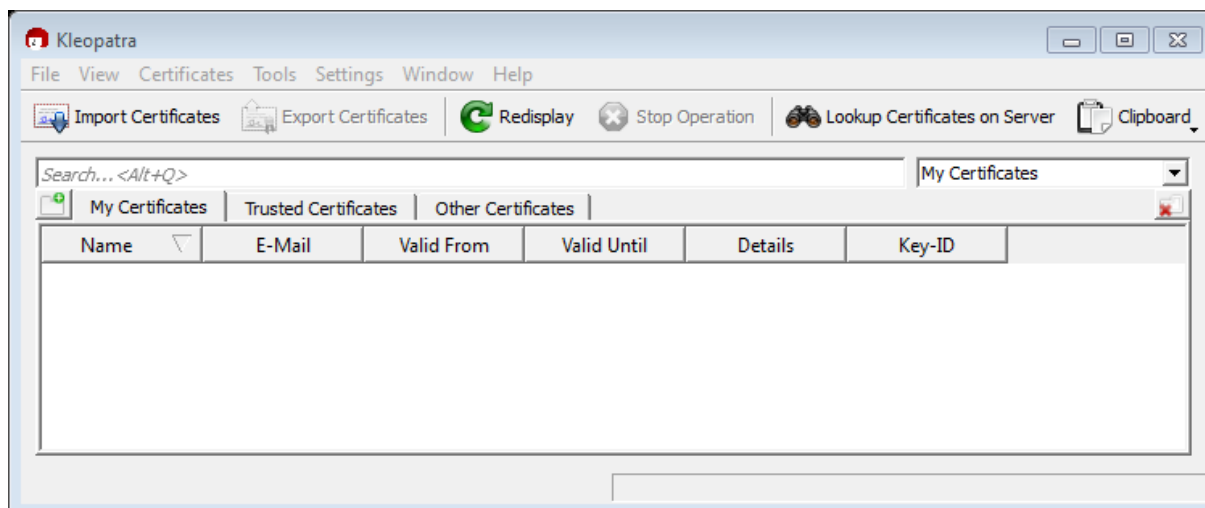
Vous obtiendrez alors l'écran suivant et pourrez *fermer*.



L'installation est donc terminée, vous pouvez désormais générer votre clé gpg.

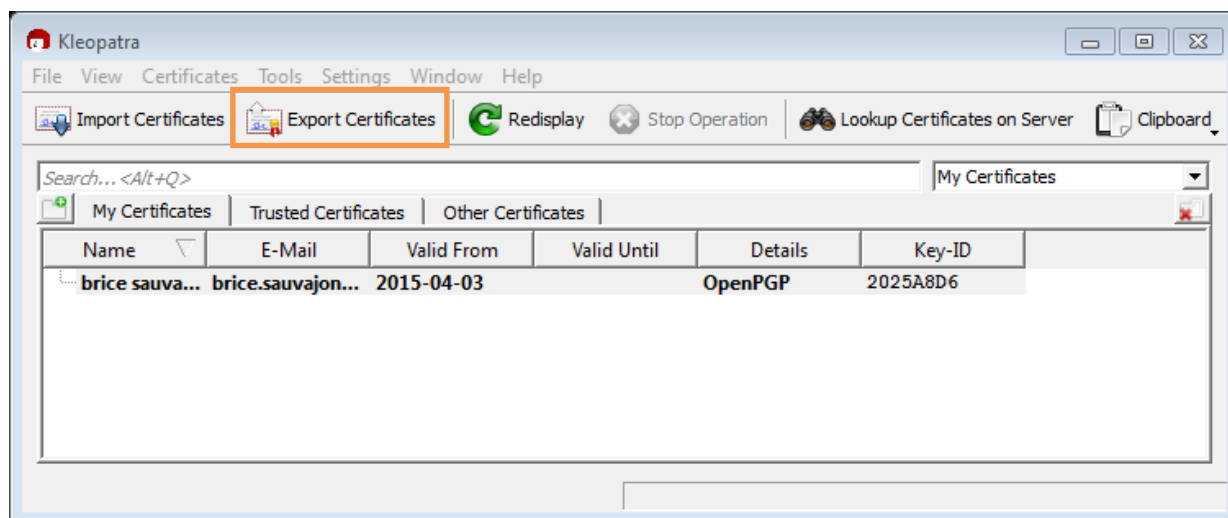
1.2 Création de la clé gpg

Depuis le menu démarrer, lancer **Kleopatra** :



1.3 Envoi de la clé à l'ATIH

Pour nous faire parvenir votre clé publique, il sera tout d'abord nécessaire de l'exporter depuis Kleopatra. Pour cela, sélectionnez votre clé puis cliquez sur « export certificate »



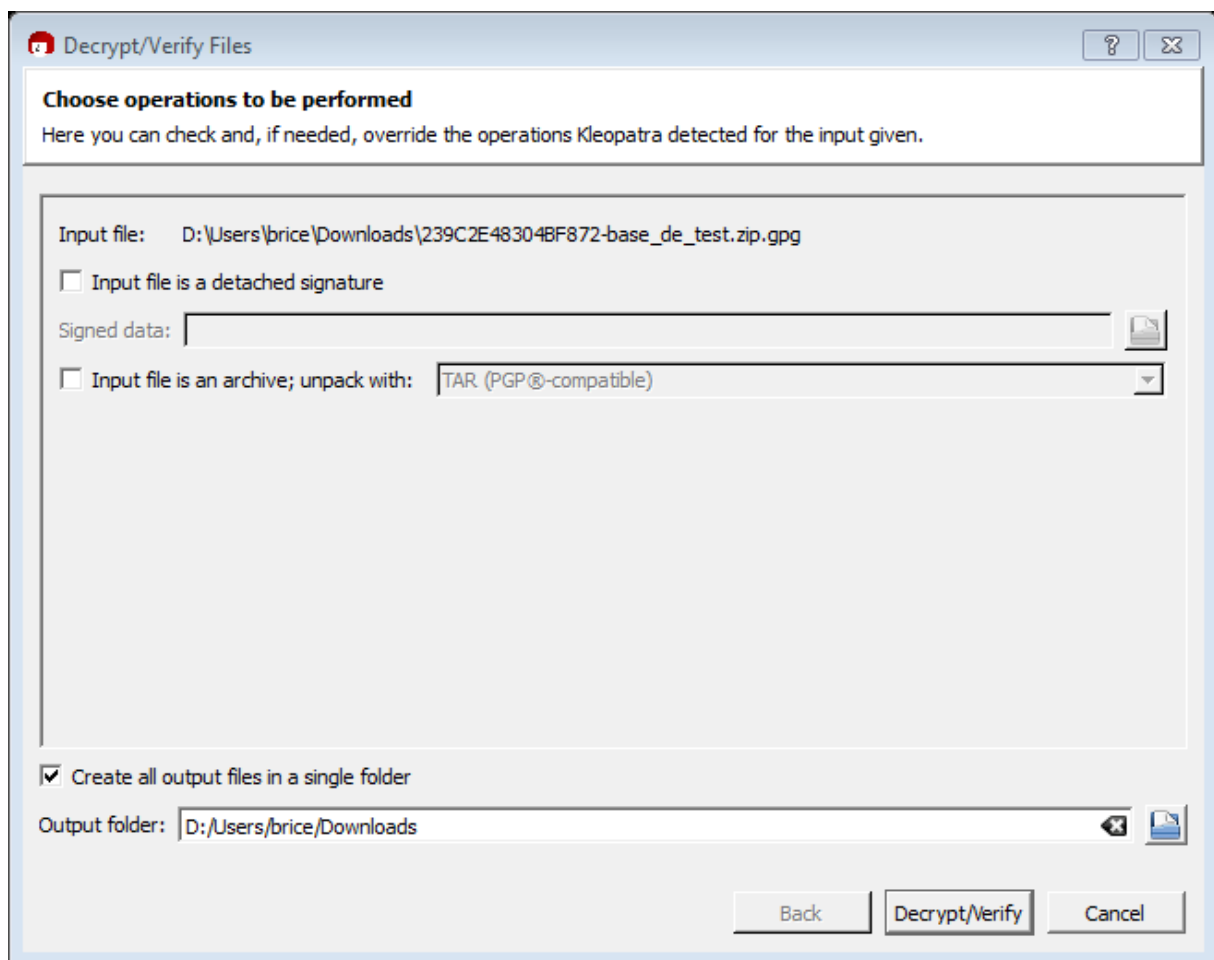
Le logiciel demandera de choisir un répertoire où enregistrer la clé au format asc. Vous devrez ensuite nous faire parvenir ce fichier par mail à destination de **demande_base@atih.sante.fr** en précisant **votre nom et votre organisation.**

2. Décryptage d'une base téléchargée

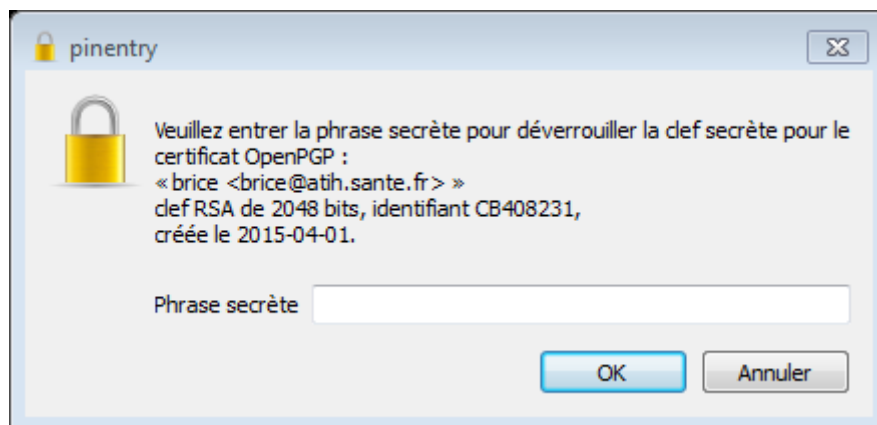
Dans Kleopatra, cliquer sur « File », puis sur « Decrypt/Verify Files », et enfin sélectionner votre fichier « .pgp ».

Dans le champ « Output folder » en bas, sélectionner le répertoire de destination de la base décryptée, puis cliquer sur « Decrypt/Verify ».

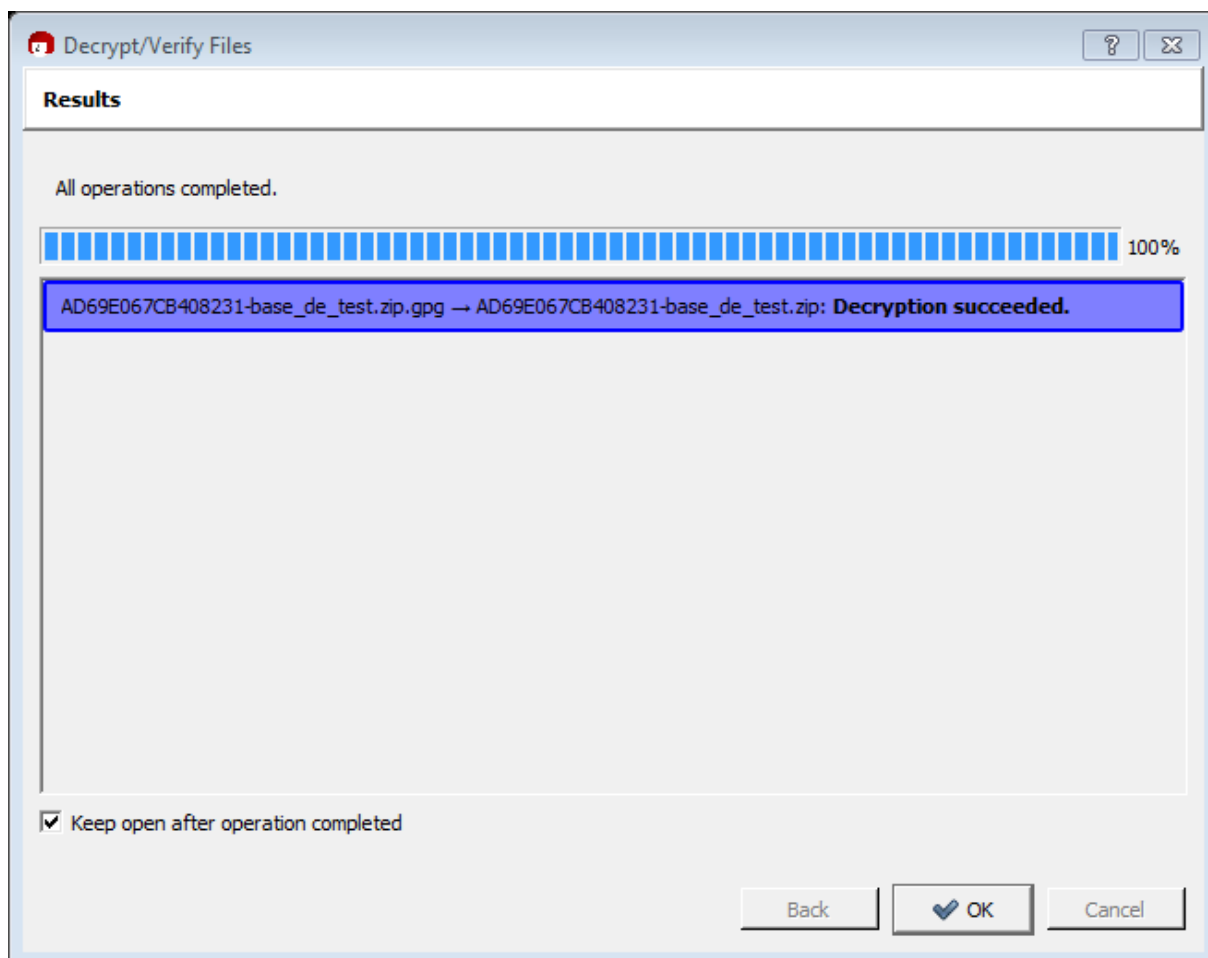
Le mot de passe de votre clé privée vous sera alors demandé.



Entrer le mot de passe de votre clé :



L'archive se décrypte alors avec votre clé privée :



Une fois terminé, vous obtiendrez un fichier au format 7z contenant toutes les données.