# Délibération n° 2009-569 du 1er octobre 2009 portant avis sur un projet de décret en Conseil d'Etat relatif à la création d'un traitement de données relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1)

01/10/2009

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le ministère de la santé et des sports, le 24 septembre 2009, d'une demande d'avis concernant un projet de décret en Conseil d'Etat relatif à la création d'un traitement de données intitulé « Traitement relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1) » ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel ;

Vu la directive 95 / 46 / CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu l'article L. 1111-8 du code de la santé publique ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et notamment ses articles 27 et 29 ;

Vu l'avis du Haut Conseil de santé publique du 7 septembre 2009 ;

Après avoir entendu M. Jean Massot, commissaire, en son rapport et Mme Elisabeth Rolin, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

La commission a été saisie, en urgence, le 24 septembre 2009, par le ministère de la santé et des sports, d'un projet de décret en Conseil d'Etat relatif à la création, par la CNAM-TS, d'un traitement de données intitulé « Traitement relatif à la gestion et au suivi des vaccinations contre la grippe A (H1N1) » sur le fondement des articles 27 (I, 1°) et 29 de la loi du 6 janvier 1978 modifiée.

Le Gouvernement a en effet confié à la CNAM-TS la prise en charge, en coordination avec l'ensemble des régimes d'assurance maladie et pour leur compte, d'un dispositif destiné, d'une part, à inviter par courrier individualisé les populations à se faire vacciner et, d'autre part, à réaliser le suivi de la montée en charge de la vaccination. Afin de remplir ces missions, il lui a été demandé de mettre en œuvre sans délai un système informatique permettant d'assurer l'organisation, la gestion et le suivi de la vaccination, de contribuer au dispositif de pharmacovigilance et d'évaluer le taux de couverture de la population.

La création d'un fichier national est rendue nécessaire en raison de l'ampleur exceptionnelle et inédite de la campagne de vaccination contre la grippe A (H1N1) décidée par le Gouvernement à la suite des recommandations de l'Organisation mondiale de la santé.

Sur les finalités :

Aux termes du projet de décret, le traitement poursuit deux finalités principales :

— l'organisation des vaccinations contre la grippe A (H1N1) ;

— la gestion et le suivi des vaccinations.

Afin de constituer le fichier des personnes invitées à se faire vacciner, les organismes d'assurance maladie obligatoire mais également d'autres organismes sociaux et certains employeurs sélectionneront, au préalable, dans leurs fichiers, leurs bénéficiaires selon les critères de priorité définis par le Gouvernement après avis du Haut Conseil de la santé publique et transmettront à la CNAM-TS, de façon progressive, les données permettant l'envoi des invitations sans qu'apparaissent les critères de sélection.

Le traitement de la CNAM-TS permettra d'adresser aux bénéficiaires de la vaccination des invitations à se faire vacciner

ainsi que des bons de vaccination préremplis (données d'identification et NIR) et des cadres à compléter concernant la vaccination. La vaccination devrait en principe être réalisée par deux injections à trois semaines d'intervalle qui devront se faire avec le même vaccin. Deux bons de vaccination seront envoyés. Le bénéficiaire devra se présenter avec l'original des bons au centre de vaccination, qui les complétera et conservera le premier bon. Le bénéficiaire conservera le second bon jusqu'à sa seconde injection.

Une fois les bons complétés par les personnels des centres de vaccination, ils seront transmis pour numérisation et enregistrement dans la base de données nationale.

Un accès distant à cette base sera possible à certains acteurs (médecins traitants, personnels habilités des organismes des régimes obligatoires d'assurance maladie et des autorités sanitaires en charge de l'organisation et du suivi de la vaccination), notamment pour l'édition de bons de vaccination dans certains cas.

La constitution de la base doit également contribuer à la pharmacovigilance et ainsi permettre la traçabilité des lots de vaccins distributifs ainsi que le signalement des éventuels effets indésirables, ce qui revêt en l'espèce un intérêt de santé publique majeur. Enfin, des statistiques anonymisées pourront être réalisées par les autorités sanitaires.

La commission considère que, eu égard à l'intérêt de santé publique que présente l'organisation de cette campagne de vaccination, la création de ce traitement et les finalités ainsi poursuivies sont adéquates et légitimes.

Sur les critères de sélection :

L'article 2 du projet de décret énumère les critères permettant aux organismes contributeurs cités dans l'article 1er (I, 1°) de sélectionner les bénéficiaires selon les ordres de priorité définis par la DGS. Or cet article précise tout de même qu'aucune donnée relative à ces critères de sélection (qui rendra prioritaire à la vaccination certains bénéficiaires) ne figurera ni sur les invitations à se faire vacciner ni sur les bons et ne sera conservée dans la base nationale.

La commission prend acte que le Gouvernement s'est engagé à modifier l'avant-dernier alinéa de l'article 2 afin de préciser que « ces critères ne sont pas transmis à la CNAM-TS par les organismes et les employeurs mentionnés au 1° du I de l'article 1er », et non « au a du 1° du 1 de l'article 1er ».

La commission estime, en tout état de cause, que, dans la mesure où ces données ne sont ni transmises ni enregistrées dans le traitement, cet article n'a pas à figurer dans le projet de décret autorisant le traitement, conformément aux dispositions de l'article 29 de la loi du 6 janvier 1978 modifiée qui énumère les éléments à faire figurer dans les actes autorisant la création d'un traitement.

Sur les données traitées :

Selon le projet de décret, seront transmises à la CNAM-TS :

1. Les données d'identification (comprenant les nom, prénom et NIR des bénéficiaires).

2. Les codes de régime d'affiliation et de l'organisme gestionnaire des bénéficiaires.

3. Les adresses de certains bénéficiaires non encore connues de la CNAM-TS, détenues par les autres régimes obligatoires d'assurance maladie (mutualité sociale agricole, régime social des indépendants...) et par d'autres organismes de sécurité sociale tels que l'ACOSS, ainsi que par les employeurs de personnes définies comme prioritaires par l'Etat en raison de leur activité professionnelle (professionnels de santé, personnels de crèches...).

La commission observe que la collecte des données d'identification (NIR, nom, prénom et date de naissance) ainsi que de l'adresse est pertinente au regard des finalités du traitement et des modalités d'organisation de la campagne.

En ce qui concerne le code du régime d'affiliation et de l'organisme gestionnaire, la seule justification de la collecte de cette donnée est que la base vaccination n'étant pas remise à jour, si la personne vaccinée à contacter a changé d'adresse, seul le régime d'affiliation peut la recontacter. La commission considère que dans ces cas, qui devraient être rares, les autorités sanitaires pourraient, conformément à l'article R. 161-37 du Code de la sécurité sociale et à l'arrêté du 22 octobre 1996 relatif au répertoire national interrégimes des bénéficiaires de l'assurance maladie (RNIAM), consulter ce répertoire qui comporte, avec une mise à jour en temps réel, le NIR, le code régime et l'organisme d'assurance maladie de rattachement. Dès lors, la commission estime que cette information n'est pas pertinente et ne doit pas figurer dans la base.

La commission prend acte qu'au regard de la finalité de suivi des vaccinations, et notamment de pharmacovigilance, les informations relatives au produit, aux dates de vaccination et à l'identification du centre et du médecin responsable de la vaccination sont pertinentes. Elle relève qu'aucune donnée relative au suivi des effets indésirables ne sera ajoutée au traitement, et donc qu'aucune donnée de santé particulièrement sensible, telle que le fait d'être atteint d'une affection de longue durée, n'est conservée.

Sur la durée de conservation :

Les données seront conservées jusqu'au 31 décembre 2012 afin d'assurer la pharmacovigilance (notamment suivi des lots, signalement des éventuels effets indésirables) puis archivées.

En outre, les informations relatives à l'identification des agents ayant accédé à la base nationale, ainsi que les dates et heures de ces accès, seront conservées pendant un an à compter de chaque accès.

La commission constate que la durée de conservation des données est proportionnée aux finalités pour lesquelles elles sont collectées et traitées.

Sur les destinataires des données :

Le projet de décret identifie trois types de destinataires.

Tout d'abord, pourront consulter la base vaccination les médecins traitants qui examineront leurs patients présentant des symptômes grippaux afin de vérifier si la personne a été vaccinée.

Dans la mesure où ces médecins ne pourront avoir accès qu'aux données concernant les patients qu'ils suivent, la commission recommande que l'article 4 du projet de décret précise que les médecins traitants seront destinataires des données « dans le cadre du suivi médical de leur patient ».

En second lieu, les agents individuellement habilités des organismes de l'ensemble des régimes obligatoires d'assurance maladie pour leurs ressortissants pourront également consulter la base vaccination à des fins notamment d'édition de bons (par exemple, en cas de perte).
Enfin, les agents individuellement habilités des autorités sanitaires en charge de l'organisation de la vaccination (centres de vaccination) pourront accéder à la base afin de vérifier l'état vaccinal des personnes qui se présentent au centre ou d'éditer à titre exceptionnel des bons de vaccination.

Sur l'établissement de statistiques et l'anonymisation des données :

Le projet de décret prévoit que des tableaux de bord permettant d'assurer le suivi du taux de couverture vaccinale soient fournis aux autorités sanitaires en charge de la gestion et du suivi du dispositif de vaccination et que les informations relatives au suivi de la vaccination mentionnées au 4° de l'article 3 soient mises à disposition de l'Agence française de sécurité sanitaire des produits de santé et de l'Institut de veille sanitaire. Or l'article 3 (4°, d) mentionne les nom et prénom du médecin responsable de la vaccination. La commission n'a pas reçu, à ce jour, de raisons convaincantes justifiant cette transmission. La commission estime que la mise à disposition de ces données à des fins d'études statistiques et épidémiologiques est parfaitement légitime. Elle demande toutefois à avoir connaissance des modalités de cette mise à disposition et en particulier des procédures mises en œuvre pour assurer l'anonymisation des données d'identification.

Sur les sécurités :

Dans la mesure où cette base de données centralisée a vocation à concerner l'ensemble de la population résidant sur le territoire français et comportera non seulement les données d'identification des personnes mais aussi leur NIR, leur adresse et des données sur la vaccination, il importe que toutes mesures soient prises pour en garantir la confidentialité.

Or, en raison de l'ampleur de l'opération et de l'impossibilité pour la CNAM-TS de mobiliser dans les temps impartis les moyens humains et matériels nécessaires, la CNAM-TS fait appel à un prestataire extérieur qui assurera la numérisation et le vidéocodage des bons de vaccination. Les données ainsi produites, qui ne comporteront pas de données de santé particulièrement sensibles, seront intégrées dans un fichier géré sur des serveurs qui sont la propriété de la CNAM-TS, mais hébergés provisoirement chez un sous-traitant du prestataire. Elle relève que cette activité de sous-traitance n'est pas soumise à la procédure d'agrément ministériel prévue par l'article L. 1111-8 du code de la santé publique, dans la mesure où elle est réalisée à l'initiative de la CNAM-TS, par ailleurs propriétaire des serveurs d'hébergement.

Dès lors, et sans méconnaître l'urgence qui s'attache à la mise en œuvre rapide de ce système d'information, la commission appelle l'attention du Gouvernement sur la nécessité de s'assurer tant par voie contractuelle que par un contrôle permanent des opérations de sous-traitance du respect des mesures de sécurité prévues pour éviter toute divulgation des données.

A cet égard, ayant procédé dans les brefs délais d'instruction qui lui étaient impartis à l'analyse des éléments de sécurité qui lui ont été communiqués à sa demande par le ministère et par la CNAM-TS, elle estime devoir formuler les constats et observations suivants :

La commission relève que le contrat de prestations comporte une clause de confidentialité par laquelle le prestataire s'engage à prendre toutes mesures pour éviter la divulgation des données qui lui sont confiées, notamment restituer

l'ensemble de la documentation remise par la CNAM-TS à l'expiration du marché et ne conserver aucune copie des documents et supports d'information, ne pas utiliser les documents et informations traitées à des fins autres que celles du marché, ne pas communiquer ces documents à d'autres personnes morales ou non, insister auprès de son personnel sur la particulière sensibilité et le caractère personnel et médical des données et rappeler l'obligation de discrétion et de confidentialité.

Elle prend également acte que l'ensemble de ces opérations seront réalisées sur le territoire français et qu'aucune donnée ne sera transférée en dehors du territoire national.

Sur les mesures de sécurité logique :

La protection du réseau contre les intrusions provenant de l'extérieur semble, en première analyse, satisfaisante. En revanche, aucun dispositif de chiffrement pour le stockage des données n'est mis en œuvre, tant au niveau de la base de données que du système d'exploitation.
Afin de répondre aux exigences de sécurité nécessaires à une base nationale contenant les NIR et les adresses de l'intégralité des bénéficiaires de l'assurance maladie, la commission estime qu'un chiffrement des données stockées sur le serveur doit impérativement être mis en place.

Sur les profils d'habilitation :

La commission préconise qu'une procédure d'authentification forte soit mise en œuvre pour les personnels des prestataires habilités à accéder au traitement (par exemple carte à puce/clé USB avec certificat et mot de passe).

Sur l'alimentation de la base de données :

La commission prend acte que les transmissions de données réalisées par les autres organismes d'assurance maladie ou sociaux ainsi que par les employeurs vers la CNAM-TS seront réalisées par envoi de fichiers cryptés.

Cependant, en ce qui concerne les liaisons entre les différents sites des prestataires et les flux d'administration, une authentification par simple mot de passe est prévue, ce qui n'est pas suffisant. En conséquence, pour garantir une bonne sécurité des échanges, la commission préconise de :

— recourir à une authentification forte (par exemple avec carte à puce/clé USB avec certificat et mot de passe) ;

— mettre en place des règles d'authentification par adresse IP (implémentés au niveau des pare-feu) devant permettre de garantir que seuls des postes bien identifiés et autorisés du prestataire peuvent établir une connexion de type administrateur sur les serveurs centraux.

La commission attire l'attention du ministère sur le fort impératif de traçabilité nécessaire à la sécurité de la « base vaccination », que ce soit pour les accès techniques ou les consultations réalisées par les destinataires.

Sur la sécurité physique :

Les éléments transmis par la CNAM-TS relatifs aux mesures de sécurité physique prises chez le sous-traitant assurant l'hébergement de la base apparaissent satisfaisants. Cependant, la commission demande à avoir connaissance des mesures de sécurité mises en œuvre sur les sites du prestataire principal et recommande en particulier que le contrôle de l'accès à ces sites soit efficient, notamment via un contrôle par badge et un système de surveillance des accès.

Sur les procédures et audits :

En ce qui concerne la procédure de traitement des supports d'information en fin de vie (disques durs, CD-ROM, etc.), la CNAM-TS a précisé qu'un effacement sécurisé était prévu. Cependant, la commission préconise que la CNAM-TS s'assure auprès de la société en charge de la numérisation et du vidéocodage que les éventuels disques durs des appareils de numérisation seront effacés de manière sécurisée ou restitués à la CNAM-TS.

Par ailleurs, la commission préconise que la CNAM-TS fasse réaliser un audit de sécurité et que des consignes de sécurité détaillées soient établies à l'attention tant des administrateurs et des techniciens que de l'ensemble des utilisateurs du système (notamment médecins, agents habilités des organismes des régimes obligatoires d'assurance maladie, autorités sanitaires en charge de la vaccination).

En conséquence la commission demande à être rendue destinataire d'un document technique complémentaire apportant des précisions sur :

— les techniques d'anonymisation ;

— la procédure de chiffrement des données stockées sur le serveur ;

— la mise en place d'authentification forte des personnes habilitées à avoir accès à la base ;

— la sécurisation de la transmission des données, notamment le recours à une authentification forte entre les différents sites des prestataires et les flux d'administration ainsi que la mise en place de règles d'authentification par adresse IP (implémentés au niveau des pare-feu) devant permettre de garantir que seuls des postes bien identifiés et autorisés du prestataire peuvent établir une connexion de type administrateur sur les serveurs centraux ;

— les mesures de sécurité physique prévues sur les sites des sociétés prestataires intervenant sur ce traitement ;

— l'effacement de manière sécurisée des éventuels disques durs des appareils de numérisation restitués à la CNAM-TS ;

— la réalisation d'un audit de sécurité et l'établissement de consignes détaillées de sécurité.

Sur l'information des personnes et l'exercice des droits d'accès et de rectification des données :

Le projet de décret précise que les droits d'accès et de rectification des données s'exercent auprès de l'organisme d'assurance maladie de rattachement de l'assuré.

Le décret prévoit que le droit d'opposition ne s'applique pas, et ce même si la vaccination est facultative. Une personne qui ne se présentera pas à la vaccination figurera tout de même dans la base en raison de l'envoi de la lettre d'invitation.

En ce qui concerne l'information des personnes, la commission prend acte que la lettre d'invitation à se faire vacciner comportera une mention précisant la finalité du traitement, les destinataires ainsi que les modalités d'exercice du droit d'accès (« Les informations recueillies sur le bon au verso sont destinées à votre organisme d'assurance maladie, aux autorités sanitaires, afin de réaliser la gestion et le suivi des vaccinations de la campagne de vaccination. Vous pouvez accéder et rectifier vos données auprès de votre organisme d'assurance maladie »).

Source : JORF n°0246 du 23 octobre 2009, texte n° 72.