

ANNEXE 4 :

LES METHODES D'ANONYMISATION DES DEMANDES DE REMBOURSEMENT ELECTRONIQUE

Remarque préalable : ce document analyse les méthodes d'anonymisation des DRE dans l'hypothèse de leur mise en œuvre sur le système SESAM Vitale en ligne. Les conclusions auxquelles elle aboutit s'appliquent cependant à une mise en œuvre dans le cadre de SESAM Vitale hors ligne.

L'anonymisation des assurés est réalisée à l'aide d'un algorithme de chiffrement stable et « non réversible », ce qui signifie que le même identifiant en entrée de l'algorithme donne toujours le même numéro d'anonymisation en sortie, d'une part, et qu'il est impossible, en raison de la non-réversibilité, de reconstituer l'identifiant d'entrée à partir du numéro d'anonymisation, d'autre part. Les bases mathématiques et les méthodes de production de tels algorithmes sont bien connues et parfaitement fiables. Elles sont notamment utilisées pour l'élaboration des signatures électroniques. L'identifiant d'entrée peut être le NIR, le numéro de contrat, l'identité de l'assuré ou toute autre donnée au choix des assureurs complémentaires, ou encore une combinaison quelconque de ces différentes données.

L'anonymisation est réalisée dans un premier temps par le tiers de confiance pour constituer la base de données du sous-système 2. Il constitue à cette occasion la table de passage entre les identifiants en clair des assurés et leurs numéros d'anonymisation. Cette table est ensuite mise à jour au fur et à mesure de la prise en compte des nouveaux assurés.

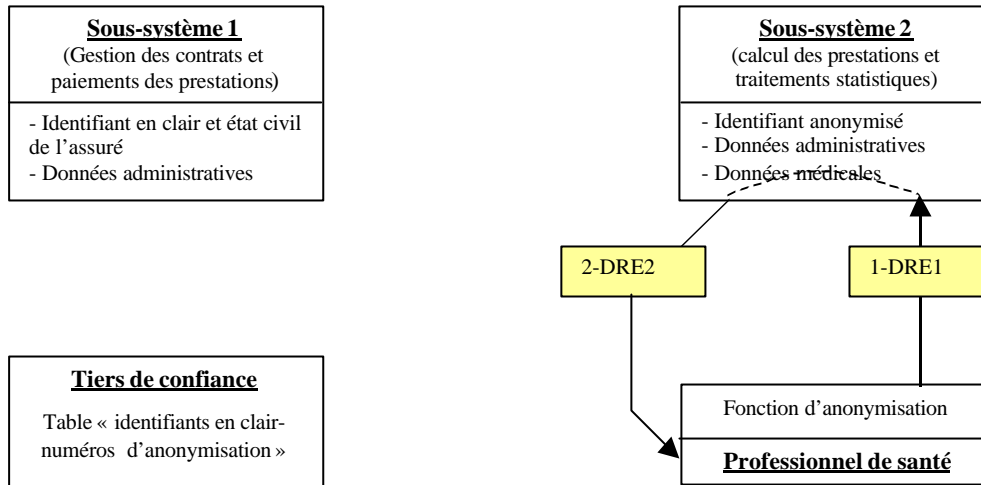
Au niveau de l'échange entre le poste du professionnel de santé et le sous-système 2, plusieurs méthodes d'anonymisation peuvent être envisagées :

- l'anonymisation par le poste du professionnel de santé ;
- l'anonymisation par le tiers de confiance ;
- l'anonymisation par la carte de l'assuré ;
- l'identification des premiers états de la demande remboursement électronique (DRE1 et DRE2) par un numéro d'ordre ou un nombre aléatoire différent du numéro d'anonymisation.

1. Anonymisation par le poste du professionnel de santé

Le même algorithme est utilisé par les professionnels de santé, pour l'émission des DRE1, et par le tiers de confiance pour l'anonymisation des assurés dans le sous-système 2.

Encadré n° 1 : Anonymisation par le poste de travail du professionnel de santé



Le poste de travail du professionnel de santé est doté du même algorithme d'anonymisation que le tiers de confiance.

- Le professionnel de santé envoie au second sous-système des DRE1 identifiées par le numéro d'anonymisation du patient-assuré.
- Le second sous-système rapproche les données des DRE ainsi anonymisées de celles du contrat de l'assuré également identifié par le numéro d'anonymisation. Il procède au calcul du montant à rembourser et retourne, en temps réel, le résultat de ce calcul au professionnel sous la forme d'un enregistrement DRE2 identifié par le numéro d'anonymisation.

Quel que soit l'algorithme retenu, il est a priori souhaitable que ce soit le même pour tous les assureurs. L'utilisation d'algorithmes différents obligerait en effet à les enregistrer tous sur les postes de travail de tous les professionnels de santé.

Cet algorithme doit être installé sur les postes de travail de tous les professionnels de santé adhérents à SESAME Vitale, soit 150 000 aujourd'hui et très probablement de l'ordre de 200 000 à échéance proche. Il doit être très soigneusement protégé car sa divulgation entraînerait la ruine du système. Le seul espace du poste de travail des professionnels de santé répondant à des normes de sécurité contrôlables est le lecteur bi-fente dans lequel le GIE a implanté les modules de certification et de chiffrement des feuilles de soins électroniques. C'est donc là que devrait être également implanté l'algorithme d'anonymisation. Mais le mode d'installation des modules de sécurisation dans le lecteur est tel que cette opération serait extrêmement malaisée¹⁷. Par ailleurs, la protection obtenue serait assez vaine. En effet, il suffirait à un tiers malintentionné de se procurer un lecteur bi-fente et de lui soumettre des identifiants en clair pour récupérer les numéros d'anonymisation correspondants.

Cette méthode

- est optimale en ce qui concerne l'efficacité du dialogue, celui-ci étant direct entre le poste du professionnel et le serveur de l'assureur ;

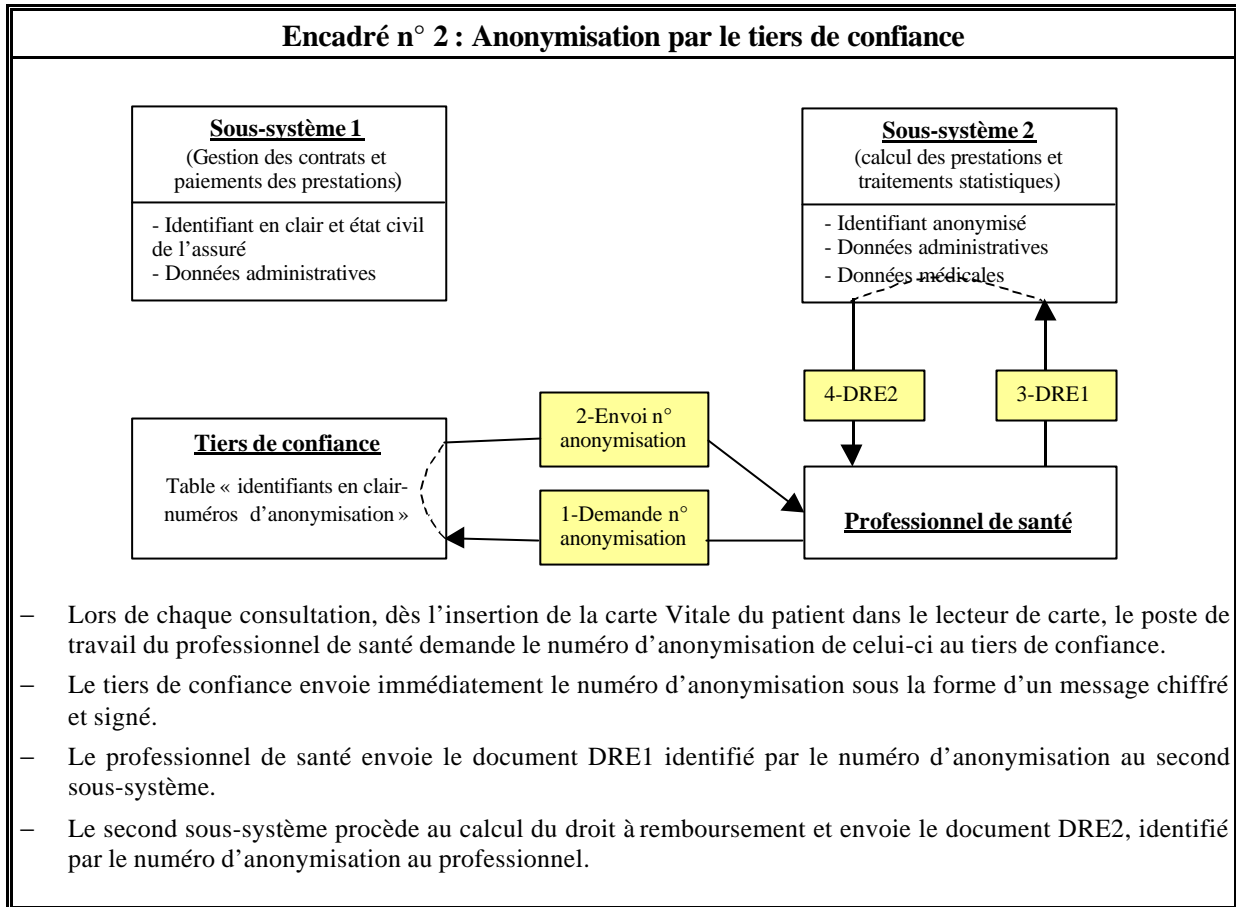
¹⁷ Les lecteurs sont fabriqués par des industriels sur la base d'un cahier des charges élaboré par le GIE. Quant au module de sécurisation, il est développé par le GIE lui-même. Les industriels n'y ont pas accès, le GIE procédant lui-même, dans leurs locaux, à son installation sur le lecteur. Se pose la question de savoir si des modifications peuvent être apportées, et par quels moyens, au module de sécurisation sur les lecteurs en service.

- n'entraîne aucune surcharge pour le professionnel de santé, ni en ce qui concerne la procédure, ni en ce qui concerne sa configuration informatique puisque l'anonymisation est réalisée dans le lecteur bi-fente ;
- ne requiert ni une évolution majeure de la carte Vitale, ni le recours à une carte supplémentaire d'assureur complémentaire ; il suffit, en effet, d'inscrire dans la carte Vitale l'identifiant de l'assureur complémentaire et le numéro du contrat, ce qui est possible dans la carte Vitale 1 actuelle ;
- mais elle est insuffisamment sécurisée pour être envisagée¹⁸, en dehors du fait qu'elle nécessiterait une mise à niveau de l'ensemble du parc de lecteurs.

2. Anonymisation par le tiers de confiance

Il s'agit d'une variante de la méthode précédente. Le poste de travail du professionnel de santé n'abrite pas de module d'anonymisation. Avant le dialogue avec le sous-système 2, il procède à un premier échange avec le tiers de confiance afin que ce dernier lui communique le numéro d'anonymisation de son patient.

¹⁸ Selon l'avant-projet de décret relatif à l'application des dispositions du dernier alinéa de l'article 8 de la loi n° 93-8 du 4 janvier 1993, le GIE SESAM Vitale devrait se voir confier l'élaboration d'un cahier des charges fixant les modalités de transmission de FSE anonymisées aux URML par les médecins conventionnés, alors que l'assurance maladie prévoyait que cette transmission se fasse en différé à partir des systèmes d'information des organismes. Le problème est de même nature que celui qui est posé ici. Le GIE n'a, à ce jour, engagé aucune étude.



Dès lors, seul le tiers de confiance détient l'algorithme d'anonymisation. Le risque de divulgation est considérablement amoindri, voire disparaît complètement d'autant qu'il n'est plus nécessaire que le même algorithme soit utilisé par tous. Chaque assureur, ou plus exactement chaque tiers de confiance peut avoir son propre algorithme dont il est seul à connaître le secret.

L'incertitude sur la capacité du GIE SESAM Vitale à déployer l'algorithme d'anonymisation sur les lecteurs de cartes des professionnels de santé est sans objet.

Mais la procédure est plus complexe car le dialogue interactif est alourdi d'une étape supplémentaire. Ceci ne constitue cependant pas un handicap significatif :

- D'une part, car cette étape peut être entièrement automatisée et être déclenchée par l'insertion de la carte du patient (SESAM vitale ou DUO) dans le lecteur sans que le professionnel de santé ait à faire d'autres manipulations ;
- D'autre part, car elle peut être réalisée dès le début de la consultation, tandis que le dialogue avec le sous-système 2, aboutissant à la production de la DRE, intervient nécessairement à la fin de la consultation, une fois connue la liste des prestations dispensées par le professionnel de santé. Le risque de dégradation des temps de réponse est par conséquent négligeable, voire nul.

3. Anonymisation par la carte de l'assuré

C'est une autre variante qui consiste à intégrer dans la carte de l'assuré, en donnée permanente, soit le module d'anonymisation, soit son numéro d'anonymisation calculé par le tiers de confiance au moment de l'adhésion auprès de l'assureur complémentaire. Le schéma de circulation de l'information est, comme avec la méthode d'anonymisation par le poste du professionnel de santé, limité à un échange entre le poste et le sous-système 2, sans intervention du tiers de confiance.

Cette méthode cumule les avantages de la première et de la seconde méthodes quant à la simplicité de la procédure, l'efficacité du dialogue et l'absence de charges pour le professionnel de santé.

Mais elle a un impact important sur la carte de l'assuré. Il importe, en effet, pour garantir la sécurité de l'anonymisation, que l'algorithme ou le numéro d'anonymisation soit enregistré dans une zone de la carte fortement protégée où l'on aura la certitude qu'il ne peut être atteint que par le truchement du module de sécurité de SESAM Vitale implanté dans le lecteur de cartes.

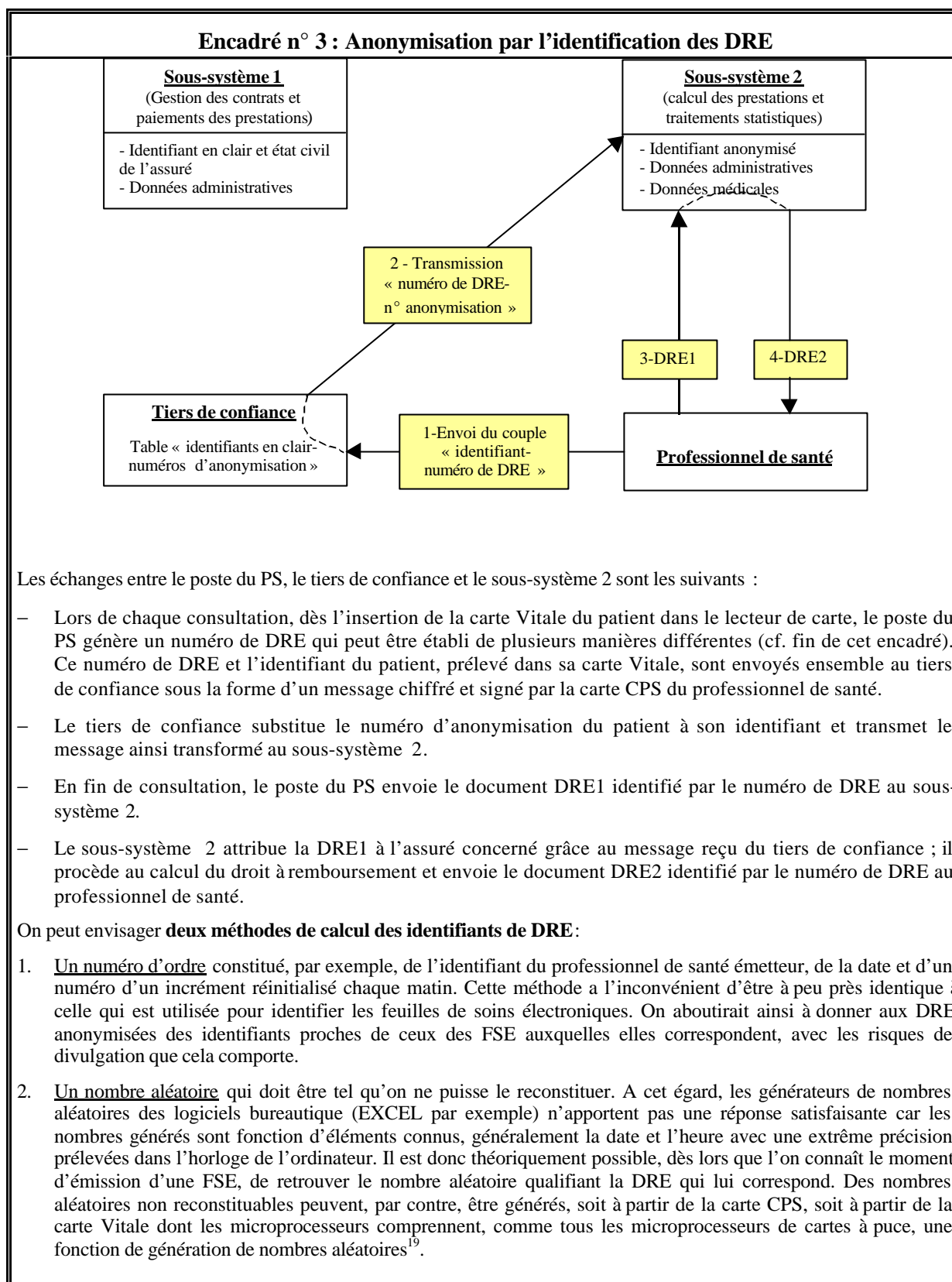
L'enregistrement du module d'anonymisation n'est pas possible avec le type de carte, Vitale 1, actuellement en service. Il ne peut être envisagé qu'avec la carte Vitale 2, soit à une échéance trop lointaine. L'enregistrement du numéro d'anonymisation, tant à l'émission de la carte (donc à la personnalisation) qu'en mise à jour, est par contre possible. Cependant sa mise en œuvre pose des difficultés industrielles, car elle nécessite la « mise en ligne » du tiers de confiance pour l'émission de la carte (le fichier de personnalisation doit comporter le numéro d'anonymisation) et en mise à jour.

In fine, la carte Vitale ne peut être réellement utilisée comme support de l'anonymisation. Il reste le recours à une carte spécifique d'assureur complémentaire qui pourrait être plus rapidement déployée. Mais cela obligerait tous les assureurs désireux d'utiliser la procédure d'anonymisation à doter leurs assurés d'une carte spécifique et les professionnels de santé à manipuler systématiquement deux cartes pour leurs patients.

Cette solution est, au total, peu satisfaisante.

4. Anonymisation par l'identification des DRE, solution à une faiblesse commune des trois solutions précédentes

Les solutions précédentes présentent toutes trois, du point de vue de la sécurité, l'inconvénient que les numéros d'anonymisation des assurés sont très fréquemment échangés entre les serveurs des assureurs complémentaires et les postes de travail des professionnels de santé. De plus, sur ces postes de travail, ils voisinent avec les identités en clair des assurés, si bien qu'il paraît a priori possible de rapprocher les uns des autres. Il existe des moyens techniques de se prémunir contre ce risque par la réalisation de l'anonymisation et du chiffrement des DRE dans une enceinte protégée, le lecteur de cartes, avant leur transmission. La fiabilité de ces moyens techniques est avérée, ils sont de même nature que ceux qui sont employés pour assurer la sécurisation de la signature électronique des FSE. Si l'une des trois premières solutions était retenue, il conviendrait d'en affiner l'analyse. Le risque serait alors qu'il apparaisse nécessaire, pour garantir un niveau de sécurité suffisant, de sortir du cadre des contraintes en matière de charges nouvelles pour les professionnels de santé.



¹⁹ Les générateurs de nombres aléatoires des cartes à microprocesseur sont basés sur des dispositifs électroniques instables (diode sensible aux bruits environnants par exemple) dont le fonctionnement n'est pas prédictible.

Un autre moyen de surmonter cette difficulté consiste à confiner la circulation des numéros d'anonymisation à l'intérieur du système d'information de l'assureur, entre le tiers de confiance et le sous-système 2, les DRE échangées entre ce sous-système et les professionnels de santé étant identifiées par un numéro d'ordre ou nombre aléatoire.

L'identification de la DRE par un nombre aléatoire est préférable à l'identification par un numéro d'ordre qui pourrait présenter le risque d'être trop proche du numéro de la FSE correspondante. Par ailleurs, des nombres aléatoires peut être aisément obtenus à partir des cartes CPS et Vitale, quelle que soit leur version, car les masques de ces cartes comportent une fonction de génération de nombres aléatoires.

Comme l'anonymisation par le tiers de confiance, cette solution alourdit le dialogue interactif d'un échange supplémentaire avec le tiers de confiance. Mais, de la même façon, cet échange peut être automatisé et il précède l'échange avec le sous-système 2 d'un laps de temps suffisant pour que cela passe inaperçu du professionnel. La génération des numéros de DRE peut être réalisée simplement à partir de tous les types de cartes avec un degré de sécurité élevé.

Cette solution est la plus sûre en ce qui concerne la sécurité de l'anonymisation des assurés car le numéro d'anonymisation reste confiné dans l'espace de l'assureur complémentaire et l'algorithme d'anonymisation n'est connu que du tiers de confiance. Si, malgré cela, ces éléments venaient à être divulgués, la responsabilité de la divulgation serait clairement établie.

La communication, du professionnel de santé au tiers de confiance, du couple constitué de l'identifiant du patient et du numéro qui identifie la demande de remboursement électronique doit être protégée par un message chiffré que seul le tiers de confiance pourra déchiffrer. Toutefois, la divulgation de ce secret, si elle s'avérait occasionnellement possible, par exemple par suite d'une négligence du professionnel émetteur, serait de peu de portée. En effet, le numéro identifiant une seule DRE, l'identification du patient concerné resterait limitée à la seule prestation décrite par cette DRE, sans que cette information puisse servir par la suite à identifier toutes les prestations dispensées à ce patient.

Variante : génération des identifiants de DRE par le tiers de confiance

On peut également confier au tiers de confiance le soin de délivrer les identifiants des DRE. Ainsi, le poste de travail du professionnel de santé ne serait pas affecté, mais le dialogue s'enrichirait d'un segment supplémentaire qui, pour les mêmes raisons que précédemment, ne pourrait affecter de façon perceptible la charge du professionnel de santé. Cette variante est, a priori, de peu d'intérêt.

5. Synthèse sur les méthodes d'anonymisation

Aucune des quatre solutions analysées n'a d'impact significatif sur la charge incombant aux professionnels de santé, ni en ce qui concerne la puissance informatique nécessaire, ni en ce qui concerne la procédure de production et d'émission des feuilles de soins électroniques.

L'anonymisation par le poste de travail du professionnel de santé comporte un risque majeur de divulgation de l'algorithme d'anonymisation auquel il n'existe apparemment pas de parade connue. Cette méthode ne peut être envisagée.

L'anonymisation par la carte de l'assuré réduit fortement, ou supprime complètement selon l'option retenue, le risque de divulgation du logiciel d'anonymisation. Mais les numéros

XVIII

d'anonymisation restent exposés. Par ailleurs, cette solution suppose une modification substantielle de la carte Vitale, qui ne saurait être réalisée à échéance acceptable, ou l'utilisation obligatoire d'une carte spécifique aux assureurs complémentaires. Cette dernière option est préconisée par certains d'entre eux, mais elle ne les satisferait pas tous. En outre, elle entraîne une complication, certes très modérée, de la procédure. Cette méthode n'est guère plus acceptable que la précédente.

L'anonymisation par le tiers de confiance ne demande ni aménagement du poste de travail du professionnel de santé, ni évolution de la structure de la carte Vitale, qui doit cependant être enrichie d'un minimum de données sur le contrat d'assurance complémentaire du porteur, ni recours à une carte spécifique d'assureur complémentaire. Elle fait par contre intervenir un acteur supplémentaire, le tiers de confiance, dans le dialogue interactif d'élaboration de la demande de remboursement électronique. Mais l'échelonnement des éléments de ce dialogue dans la durée de la consultation est tel que cela ne devrait pas avoir d'effet perceptible par le professionnel de santé. Le problème de la protection des numéros d'anonymisation, très fréquemment échangés sur le réseau, reste cependant posé.

L'anonymisation par l'identification des DRE à l'aide d'un nombre aléatoire supprime ce dernier problème. Comme l'anonymisation par le tiers de confiance, elle est sans impact sur la carte. Le dialogue d'élaboration de la DRE présente des caractéristiques identiques, avec aussi peu d'effet sur la charge du professionnel de santé. C'est la solution la plus pertinente.