Ordonnance
sur les standards minimaux auxquels doivent satisfaire les mesures techniques et organisationnelles à prendre par les services et institutions utilisant systématiquement le numéro d'assuré AVS en dehors de l'AVS

du xxxxx *Projet de juin 2007*

Le Département fédéral de l'intérieur,

vu l'art. 50*g*, al. 3, de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants (LAVS)[1],
en accord avec le Département fédéral des finances,

arrête :

Section 1 Dispositions générales

Art. 1 Objet

La présente ordonnance vise à garantir que les services et institutions habilités à utiliser systématiquement le numéro d'assuré prennent des mesures techniques et organisationnelles suffisantes pour :

a. s'assurer que le numéro utilisé est correct ; et
b. en prévenir toute utilisation abusive.

Art. 2 Champ d'application

La présente ordonnance s'applique à tous les services et institutions qui utilisent le numéro d'assuré conformément aux art. 50*d* et 50*e* LAVS.

Section 2 Spécifications techniques

Art. 3 Stockage du numéro d'assuré

Le numéro d'assuré ne doit être stocké qu'à un seul endroit dans une même banque de données.

[1] RS **831.10**

Art. 4 Saisie manuelle du numéro d'assuré

1 Le numéro d'assuré ne peut être saisi manuellement dans un fichier de données électroniques qu'après vérification de la clé de contrôle suivant la procédure décrite à l'annexe 1.

2 La lecture optique du numéro sous forme de code barre est assimilée à une saisie manuelle.

Section 3 Mesures visant à garantir l'utilisation du bon numéro d'assuré

Art. 5 Sûreté de la source des données saisies

1 Lors de la première mise à jour complète de leurs fichiers électroniques de données, les services tenant les registres visés par l'art. 2 de la loi fédérale du 23 juin 2006 sur l'harmonisation de registres[2] et les assureurs au sens de l'art. 11 de la loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal)[3] doivent ne saisir le numéro d'assuré que s'il leur a été communiqué par une procédure conforme à l'art. 134^{quater}, al. 2 ou 4, du règlement du 31 octobre 1947 sur l'assurance-vieillesse et survivants (RAVS)[4]. Pour les autres saisies, les al. 2 à 4 s'appliquent par analogie.

2 Les autres services et institutions autorisés ne peuvent saisir le numéro d'assuré dans des fichiers électroniques de données que si la certitude quant à l'exactitude du numéro est suffisante.

3 La certitude quant à l'exactitude du numéro d'assuré est réputée suffisante lorsque ce dernier a été communiqué par une procédure conforme à l'art. 134^{quater}, al. 2 ou 4, RAVS.

4 Il est permis de supposer que la certitude est suffisante lorsqu'il n'existe aucun doute sur l'identité de la personne correspondant au numéro d'assuré que l'on s'apprête à saisir et que la source du numéro est l'une des suivantes :

a. certificat d'assuré AVS au sens de l'art. 135bis RAVS ;

b. carte d'assuré au sens de l'art. 42*a* LAMal valable au moment de la saisie ;

c. communication par écrit ou par voie électronique, d'actualité au moment de la saisie, émanant d'un organe de l'AVS ;

d. communication par écrit ou par voie électronique, d'actualité au moment de la saisie, émanant d'un service ou d'une institution recommandés par la CdC comme étant suffisamment sûrs.

5 La CdC publie sur Internet la liste des services et institutions qu'elle recommande comme étant suffisamment sûrs au sens de l'al. 4, let. d.

2 RS **431.02**
3 RS **832.10**
4 RS **831.101**

Art. 6 Vérification des numéros d'assuré saisis

[1] Les services et institutions visés par l'art. 5, al. 1, vérifient périodiquement, pour tous les numéros d'assuré saisis, s'ils concordent avec les données personnelles importantes pour l'attribution du numéro. Cette vérification suit la procédure définie à l'art. 134^{quater}, al. 2 ou 4, RAVS.

[2] Si la CdC a lieu de penser qu'un service ou une institution utilise un numéro d'assuré qui n'est pas exact, elle ordonne une vérification.

Section 4 Mesures visant à prévenir toute utilisation abusive

Art. 7 Principes

[1] L'accès aux fichiers électroniques contenant le numéro d'assuré n'est accordé qu'aux personnes qui ont besoin dudit numéro pour remplir leurs tâches. Les droits de lecture et d'écriture dans lesdits fichiers est réservé à ces personnes.

[2] Lorsque le numéro d'assuré est utilisé de manière systématique dans des systèmes complexes, les mesures de protection nécessaires sont prises sur la base d'une analyse détaillée des risques.

[3] L'utilisation de ressources informatiques et de supports de données se conforment aux prescriptions minimales de sécurité définies dans l'annexe 2.

Art. 8 Transmission de données par les réseaux publics

Lorsque des jeux de données contenant le numéro d'assuré transitent par un réseau public, ils sont cryptés conformément à l'état de l'art.

Art. 9 Utilisation et communication

Les services et institutions qui utilisent le numéro d'assuré veillent à informer leurs collaborateurs, dans le cadre de cours de formation et de perfectionnement, que le numéro d'assuré ne peut être utilisé qu'en rapport avec leurs tâches et ne peut être communiqué que conformément aux prescriptions légales.

Art. 10 Entrée en vigueur

[1] La présente ordonnance entre en vigueur le xxxxxx, sous réserve des al. 2 et 3.

[2] L'art. 5, al. 4, let. a, entre en vigueur le 1er juillet 2008.

[3] L'art. 5, al. 4, let. b, entre en vigueur le 1er janvier 2009.

xxx.xxx.2007 Département fédéral de l'intérieur :

Pascal Couchepin

Annexe 1

Vérification de la clé de contrôle (art. 4)

A. Composition du numéro d'assuré

x_{n-12}	x_{n-11}	x_{n-10}	.	x_{n-9}	x_{n-8}	x_{n-7}	x_{n-6}	.	x_{n-5}	x_{n-4}	x_{n-3}	x_{n-2}	.	x_{n-1}	x_n
Code pays				**Numéro de neuf chiffres**											**Clé de contrôle**
7	**5**	**6**		**1**	**2**	**3**	**4**		**5**	**6**	**7**	**8**		**9**	**7**

B. Logique de la clé de contrôle

La clé de contrôle est le dernier chiffre du numéro (x_n) ; elle s'obtient par les opérations suivantes :

- multiplier alternativement par 3 et par 1 chaque chiffre, en commençant par l'avant-dernier (x_{n-1}), et additionner ces produits :

  total intermédiaire $= (3x_{n-1}) + (x_{n-2}) + (3x_{n-3}) \ldots$.

- déterminer ensuite la valeur (clé de contrôle x_n) qui, ajoutée au total intermédiaire, donnera le prochain multiple de 10.

Remarque:

Si le total intermédiaire est déjà un multiple de 10, la clé de contrôle est 0.

C. Illustration

Numéro d'assuré	**7**	**5**	**6**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**→ ? ←**
Multiplicateur	1	3	1	3	1	3	1	3	1	3	1	3	
Résultat	7	15	6	3	2	9	4	15	6	21	8	27	← total intermé-diaire : 123
Valeur à ajouter pour obtenir un multiple de 10	130 est le prochain multiple de 10 après le total intermédiaire 123. La différence, et donc la clé de contrôle, est 7 →												**? = 7**

Annexe 2

Prescriptions minimales de sécurité à respecter dans l'exploitation de ressources informatiques et de supports de données employés en lien avec l'utilisation systématique du numéro d'assuré

1. L'accès aux ressources informatiques et aux unités de mémoire est sécurisé physiquement. En cas d'usage de ressources informatiques et de supports de données mobiles, on veillera par des procédés cryptographiques (codage de données) conformes à l'état de l'art à rendre impossible l'accès et l'utilisation par des personnes non autorisées.

2. L'accès aux ressources informatiques et aux unités de mémoire est protégé par des mesures de sécurité informatique appropriées et correspondant aux dernières possibilités techniques et aux risques encourus. Ces mesures comprennent au moins l'emploi de logiciels (antivirus), disponibles dans le commerce et régulièrement mis à jour, de détection et d'élimination des maliciels, et le recours à des systèmes de pare-feu (centraux ou individuels).

3. Les utilisateurs ayant accès aux ressources informatiques et aux unités de mémoire doivent s'authentifier. Si l'authentification se fait au moyen d'un mot de passe, celui-ci remplit les conditions suivantes :
   a. Longueur
      - 8 caractères au moins
   b. Composition
      - Majuscules, minuscules, chiffres, caractères spéciaux
      - Au moins deux de ces catégories sont représentées
      - Eviter les mots de passe banals tels que nom, prénom, date de naissance, ID d'utilisateur, etc.
   c. Validité
      - S'il y a lieu de penser que des personnes non autorisées connaissent un mot de passe, celui-ci est changé immédiatement.
   d. Communication
      - Le mot de passe est tenu secret et ne peut être communiqué.

4. Les mises à jour d'élimination des erreurs (patches de débogage) sont appliquées aussitôt que possible aux systèmes d'exploitation et aux logiciels.

5. Sur les systèmes informatiques employés, les responsables consignent par écrit les activités et événements importants et les analysent régulièrement.

6. La reconstitution des données perdues et la possibilité de les réutiliser sont décrites dans un concept de sauvegarde des données et font régulièrement l'objet d'exercices.

7. Lorsqu'une ressource informatique ou une unité de mémoire doit être réparée, éliminée ou détruite, il est impératif qu'elle ne contienne plus de numéros d'assuré et que ceux-ci ne puissent pas être reconstitués.