

RÉFÉRENTIELS

# Algorithme de calcul de l'INS-C

Programme Identifiant National de Santé - **V1.1** - Février 2014





# SOMMAIRE

<b>SOMMAIRE .....</b>	<b>3</b>
<b>1. INTRODUCTION.....</b>	<b>5</b>
1.1. Contexte	
1.2. Objet	
<b>2. SPÉCIFICATIONS DE L'INS-C .....</b>	<b>6</b>
2.1. Principe général de calcul de l'INS-C	
2.2. Format de l'INS-C	
2.3. Normalisation des données	
2.3.1. Caractères acceptés en entrée de la fonction de calcul de l'INS-C	
2.3.2. Normalisation des caractères	
2.3.3. Traitement des champs vides	
2.4. Algorithme de calcul de l'INS-C	
2.4.1. Données en entrée	
2.4.2. Contrôle avant calcul	
2.4.3. Normalisation des champs avant calcul	
2.4.4. Algorithme de calcul de l'INS-C	
<b>3. ANNEXE 1 : EXEMPLES DE CODES DE CALCUL DE L'INS-C.....</b>	<b>11</b>



# 1. INTRODUCTION

## 1.1. Contexte

Pour répondre à leurs besoins de conservation, voire d'échange et de partage de données de santé, plusieurs régions ont développé des solutions d'attribution d'identifiants de patients. Les principes retenus permettent une génération distribuée des identifiants de patient, au niveau des LPS.

Ces principes étant différents selon les projets, l'échange et le partage de données de santé entre régions nécessitent la mise en place d'accords bilatéraux et de mécanismes de rapprochement d'identité des patients souvent complexes et débordant du périmètre de responsabilité des acteurs impliqués.

Le déploiement de l'identifiant national de santé attribué par un système central permettra de sécuriser le contenu des échanges (la bonne donnée pour le bon patient), en garantissant les qualités attendues de cet identifiant. Cet INS géré par un système central est l'INS cible.

Dans l'attente de l'INS cible, un algorithme partagé de génération d'identifiant permet d'apporter une amélioration immédiate à la situation actuelle. Les identifiants ainsi calculés sont appelés INS-C (INS Calculé).

L'INS-C constitue le premier palier de mise en œuvre de l'identifiant national de santé.

## 1.2. Objet

Le choix d'une génération répartie des INS-C impose un processus basé sur un algorithme unique partagé et connu de tous les acteurs, permettant une intégration facile dans les outils des professionnels de santé.

Par définition, ce processus ne peut être un processus aléatoire car il doit être reproductible et doit se fonder sur des critères discriminants disponibles pour les systèmes devant générer l'INS-C.

Ce document est le document de spécifications de l'algorithme pour le calcul de l'INS-C.

La définition des spécifications de l'INS-C s'appuie sur les travaux de l'ANSSI.

## 2. SPÉCIFICATIONS DE L'INS-C

### 2.1. Principe général de calcul de l'INS-C

L'INS-C est obtenu en appliquant un algorithme défini par le ministère de la santé et le concours de l'ANSSI à un nombre limité de traits d'identité de la personne concernée.

Les traits d'identité retenus sont les suivants :

- Le NIR de la personne concernée ;
- Le prénom de la personne concernée ;
- La date de naissance de la personne concernée.

Il faut utiliser les valeurs **lues dans les champs de la carte Vitale** correspondant à ces données. L'algorithme de calcul est spécifié plus loin dans le présent document.

Il s'agit des traits d'identité de la personne concernée (bénéficiaire ayant droit ou ouvrant droit) et non de son ouvrant droit si la personne concernée est un ayant-droit.

Il est obligatoire d'utiliser les traits lus de la carte Vitale.

### 2.2. Format de l'INS-C

L'INS-C est composé de 20 caractères numériques auquel s'ajoute une clé de contrôle de 2 chiffres.

Exemple : 15489609345890393434 76

1 548 960 934 589 039 343 4	76
INS calculé	clé de contrôle

La clé de contrôle est calculée selon la même règle que la clé du NIR : la clé est égale au complément à 97 du reste de la division euclidienne de l'INS calculé par 97.

## 2.3. Normalisation des données

Les traits d'identité doivent, si nécessaire, faire l'objet d'une normalisation avant le calcul.

### 2.3.1. Caractères acceptés en entrée de la fonction de calcul de l'INS-C

L'algorithme de calcul de l'INS-C n'accepte en entrée que les caractères alphanumériques encodés au format ASCII définis dans le tableau suivant. Pour information, cette définition est celle du type de données « CA : Caractères alphanumériques » définie dans le manuel de programmation des services SESAM-Vitale 1.40.x

Type de données	Caractères	Encodage ASCII correspondant
CA	Chiffres de '0' à '9'	'0' [0x30] à '9' [0x39]
	Lettres alphabétiques majuscules non accentuées ['A' à 'Z']	'A' [0x41] à 'Z' [0x5A]
	Espace	' ' [0x20]

### 2.3.2. Normalisation des caractères

Quel que soit l'encodage d'origine des données (ISO-8859-1, EBCDIC, autres), les caractères constitutifs des données doivent être normalisés selon les règles décrites dans les tableaux suivants.

Caractère d'origine quelque soit l'encodage. Les caractères présentés dans le présent tableau sont ceux retenus par le standard ISO 8859-1	Valeur normalisée de remplacement du caractère.	Encodage ASCII
Caractères alphabétiques minuscules non accentués ('a' à 'z')	Caractère alphabétique majuscule correspondant non accentué	'A' [0x41] à 'Z' [0x5A]
Caractères majuscules non accentués ('A' à 'Z')	Caractère alphabétique majuscule correspondant non accentué	'A' [0x41] à 'Z' [0x5A]
Caractère accentués : À Á Â Ã Ä Å Æ à á â ã ä å æ ã ä å	A majuscule	'A' [0x41]
Caractère accentués : Ê Ë Ì Í Î Ï Ñ Ò Ó Ô Õ Ö Ø Ù Ú Û Ü Ý Þ à á â ã ä å æ ç è é ê ë ì í î ï ñ ò ó ô õ ö ø ù ú û ü ý þ ÿ	E majuscule	'E' [0x45]
Caractère accentués : Ð ð	D majuscule	'D' [0x44]
Caractère accentués : Ò Ó Ô Õ Ö Ø Ù Ú Û Ü Ý Þ à á â ã ä å æ ç è é ê ë ì í î ï ñ ò ó ô õ ö ø ù ú û ü ý þ ÿ	O majuscule	'O' [0x4F]
Caractère accentués : Ý ý ÿ	Y majuscule	'Y' [0x59]
Caractère accentués : Ç ç	C majuscule	'C' [0x43]
Caractère accentués : Ì Í Î Ï Ñ Ò Ó Ô Õ Ö Ø Ù Ú Û Ü Ý Þ à á â ã ä å æ ç è é ê ë ì í î ï ñ ò ó ô õ ö ø ù ú û ü ý þ ÿ	I majuscule	'I' [0x49]
Caractère accentués : Ñ ñ	N majuscule	'N' [0x4E]
Caractère accentués : Ù Ú Û Ü Ý Þ à á â ã ä å æ ç è é ê ë ì í î ï ñ ò ó ô õ ö ø ù ú û ü ý þ ÿ	U majuscule	'U' [0x55]
Caractère accentués : ß	B majuscule	'B' [0x42]
Tous les autres caractères (! « # \$ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` {   } ~ NBSP ¡ ¢ £ ¤ ¥ ¦ § ¨ © ª « ¬ ® ¯ ° ± ² ³ ´ µ ¶ · ¸ ¹ º » ¼ ½ ¾ ³/⁴ ½ × ÷ þ ÷ þ	Caractère Espace	' ' [0x20]

### Cas des caractères non pris en charge par la norme ISO8859-1 :

Caractère d'origine quelque soit l'encodage.	Valeur normalisée de remplacement	Encodage ASCII
Œ et œ	OE	'OE' [0x4F, 0x45]
Š š	S	'S' [0x53]
Ž ž	Z	'Z' [0x5A]
Ÿ	Y	'Y' [0x59]
Tout autre caractère	Caractère Espace	' ' [0x20]

#### Remarque sur le format des données

L'objectif de la normalisation des données est d'avoir une représentation identique des données quelle que soit l'origine des données. Ainsi, le choix s'est porté vers une simplification des caractères (l'hypothèse est d'avoir un minimum d'impact sur les logiciels de PS et donc ne pas imposer le support de jeux de caractères plus complexes que l'ASCII).

#### 2.3.3. Traitement des champs vides

Si le champ prénom est vide, il doit être renseigné au moins par un caractère espace en entrée de la fonction de calcul de l'INS-C.

Si le champ date de naissance est vide, il doit être renseigné à la valeur 000000 en entrée de la fonction de calcul de l'INS-C.



## 2.4. Algorithme de calcul de l'INS-C

### 2.4.1. Données en entrée

Il s'agit des données dont les caractères ont été normalisés selon les règles exposées au chapitre précédent.

Ces données sont celles de la personne dont on souhaite calculer l'INS.

Données	Format	Description
NIR	CA	NIR de la personne (13 caractères)
Clé du NIR	CA	Clé du NIR de la personne (2 caractères)
Prénom	CA	Prénom de la personne
Date de naissance	CA	Date de naissance de la personne au format AAMMJJ

### 2.4.2. Contrôle avant calcul

Un contrôle de cohérence entre le NIR et la clé du NIR doit être fait avant le calcul de l'INS-C. En cas d'incohérence entre le NIR et la clé du NIR, le calcul de l'INS-C est abandonné.

Le calcul est également abandonné si le NIR correspond à un NIR temporaire.

### 2.4.3. Normalisation des champs avant calcul

#### NIR

Les 13 caractères alphanumériques du NIR sont utilisés. La clé du NIR est utilisée pour contrôler la valeur du NIR.

#### Prénom

Si le champ prénom de la carte Vitale du patient contient plusieurs prénoms (un prénom composé par exemple), il s'agit dans une première étape de supprimer tous les espaces, puis de retenir les 10 premiers caractères de la chaîne ainsi obtenue. Si la chaîne résultante est constituée de moins de 10 caractères, elle est complétée à droite par des espaces (0x20).

#### 2.4.3.1. Date de naissance

Le format AAMMJJ sur 6 caractères numériques est utilisé.

#### 2.4.4. Algorithme de calcul de l'INS-C

1. Récupérer les données nécessaires au calcul : NIR, prénoms et date de naissance de la personne concernée.  
Ces données doivent être issues de la dernière lecture de carte Vitale et avoir été conservées dans le dispositif de lecture de manière intègre.
2. Normaliser les données selon les règles énoncées plus haut dans l'ordre suivant :
  - a. normalisation des caractères
  - b. puis normalisation des champs.
3. Concaténer sans séparateur les trois champs dans l'ordre suivant : Prénom, date de naissance puis NIR.  
L'ensemble concaténé constitue la « graine ».  
Graine = Prénom (10 caractères) + Date de naissance (6 caractères) + NIR (13 caractères).
4. Calculer le haché de la chaîne de caractère 'Graine' au moyen de la fonction SHA256 (cf. le référentiel cryptographique de l'ANSSI).  
Le résultat obtenu est une empreinte de 256 bits.
5. Conversion de l'empreinte en format numérique (chiffres de 0 à 9)  
Les 64 bits de poids fort de l'empreinte sont convertis en base 10 afin d'obtenir une chaîne composée de 20 chiffres. Si le nombre obtenu s'exprime sur moins de 20 chiffres, il est complété à gauche par des zéros.
6. Calcul de l'INS-C  
L'INS-C est constitué du nombre de 20 chiffres obtenu à l'étape précédente complété par une clé de contrôle sur 2 chiffres.  
La clé de contrôle est calculée selon la même règle que la clé du NIR : la clé est égale au complément à 97 du reste de la division euclidienne du nombre de 20 chiffres par 97.
7. Après le calcul de l'INS-C, supprimer les données utilisées pour le calcul de l'INS-C qui ne sont pas nécessaires au logiciel (en particulier le NIR, sauf usage prévu aux articles R115-1 et R115-2 du Code de la sécurité sociale).

### 3. ANNEXE 1 : EXEMPLES DE CODES DE CALCUL DE L'INS-C

Les exemples de codes sont publiés dans le document [ASIP\_ProgrammeINS\_Dossier\_de\_concep-tion\_INS-C\_Exemples\_de code\_v1.0.0.pdf].



Agence des systèmes d'information partagés de santé  
9, rue Georges Pitard – 75015 Paris  
T. 01 58 45 32 50  
[esante.gouv.fr](http://esante.gouv.fr)