Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI

Office fédéral de la santé publique
Division Stratégies de la santé

21 septembre 2023

Concept d'identificateur de personnes

Résultats du groupe de travail Concept d'identificateur de personnes

Référence du dossier : 221-169/2/5

Remarque :
Ce document présente le résultat des discussions qui ont eu lieu au sein du *Groupe de travail Concept d'identificateur de personnes faisant partie* du *groupe spécialisé Gestion des données dans le système de santé* entre le 13 mars 2023 et le 18 septembre 2023. Les résultats documentés dans ce concept ne reflètent pas la position officielle des organisations participant au GT (y compris l'OFSP et la CDS).

Contenu

Liste des abréviations

GT CIP	Groupe de travail Concept d'identificateur de personne
AVS	Assurance-vieillesse et survivants
NAVS	Numéro AVS
LPD	Loi fédérale sur la protection des données
PFPTD	Préposé fédéral à la protection des données et à la transparence
DEP	Dossier électronique du patient
LDEP	Loi fédérale sur le dossier électronique du patient
EPR-SPID	Caractéristique d'identification du patient du DEP
GGDS	Groupe spécialisé Gestion des données dans le système de santé
GSRN	Global Service Relation Number
IES NG	Système d'information et d'exploitation de nouvelle génération
LAI	Loi fédérale sur l'assurance-invalidité
SIH	Système informatique hospitalier
LAMal	Loi fédérale sur l'assurance-maladie
IP	Identificateur personnel
SIC	Système informatique des cabinets médicaux
CSI	Conférence suisse sur l'informatique
UPI	Unique Person Identification (système informatique de la CdC pour la gestion des identificateurs personnels. Actuellement: NAVS et EPR-SPID)
LAA	Loi fédérale sur l'assurance-accidents
LCA	Loi fédérale sur le contrat d'assurance
CdC	Centrale de compensation

1 Contexte

L'identification sûre et biunivoque des personnes est indispensable pour de nombreux processus et aspects de la gestion du système de santé (y c. la recherche). Certes, dans la plupart des cas, l'identification des personnes peut théoriquement se faire à l'aide de caractéristiques comme le nom, le lieu de domicile, la date de naissance, etc. Mais ce type d'identification est tributaire de la qualité des données. Les sources d'erreur sont, par exemple, les noms étrangers complexes contenant des caractères spéciaux ou des lettres non latines, les confusions entre le nom de famille et le nom de célibataire ou les erreurs de transcription pour des noms phonétiquement identiques, mais s'écrivant différemment. Dans le contexte des systèmes informatiques, l'identification au moyen de caractéristiques démographiques s'avère plus complexe et génère plus d'erreurs que l'utilisation d'un identificateur personnel biunivoque (IP). L'interopérabilité dans le système sanitaire ne peut être garantie que si les objets et les personnes peuvent être identifiés de manière biunivoque, quels que soient des systèmes. L'introduction d'un IP biunivoque est donc indispensable. Il contribue également à la sécurité des patients dans la mesure où il réduit à un minimum le risque d'une attribution erronée, p. ex. de résultats d'examens ou d'une médication. De même, un IPU est très utile pour la bonne personne des données provenant de sources diverses ou saisies à des moments différents. À titre d'exemple :

- la fusion[1] de données dans le système informatique hospitalier (SIH) d'un établissement d'une certaine taille comprenant plusieurs services ou cliniques ;
- la fusion de données pertinentes pour le traitement et provenant de différents systèmes primaires (système informatique hospitalier [SIH] et système informatique des cabinets médicaux [SIC]) dans le dossier électronique du patient (DEP) ;
- la fusion des données de facturation d'un assuré par l'assureur-maladie ;
- la fusion de données provenant de différentes sources par les registres cantonaux des tumeurs ainsi que la fusion de ces données au niveau national à des fins d'analyse ;
- la fusion des informations concernant une personne ou un cas en particulier dans les systèmes de déclaration pour la surveillance de maladies infectieuses ;
- la fusion d'informations relatives à des personnes dans des registres de qualité et de dispositifs médicaux[2]
- le suivi en temps réel des capacités hospitalières dans le Système d'information et d'exploitation de nouvelle génération (IES NG) via l'appariement des capacités hospitalières et l'affectation des patients à admettre ;
- l'appariement de jeux de données provenant de sources diverses à des fins de recherche.

Avec le *Rapport concernant l'amélioration de la gestion des données dans le domaine de la santé*, le *Rapport du Conseil fédéral donnant suite au postulat 15.4225 Humbel* et la *Motion 21.4373 Introduction d'un identificateur biunivoque des patients*, le Conseil fédéral et le Parlement ont adopté trois mandats visant à promouvoir l'introduction d'un identificateur personnel biunivoque dans le système de santé.

2 Mandat du GT Concept d'identificateur de personnes

Le *groupe spécialisé Gestion des données dans le domaine de la santé (GGDS)* a chargé le GT Concept d'identificateur de personnes (GT CIP) d'élaborer une proposition pour l'introduction d'un identificateur personnel biunivoque dans le système de santé. Dans ce cadre, le présent concept a été développé en concertation avec les autorités concernées à l'échelon de la Confédération et des cantons ainsi qu'avec d'autres acteurs du système de santé. Il met en évidence, pour les différents cas d'utilisation, les indicateurs personnels existants ou manquants et propose une solution cohérente pour tous

[1] Par « fusion », on entend ici, d'une part, l'appariement des données concernant une personne et provenant de différentes sources et, d'autre part, l'attribution de données à une personne identifiée de manière univoque.

[2] Par registre médical, on entend un « relevé systématique, au sein d'un secteur d'activité prédéterminé, de données relatives à une population ou à des patients, mais également de données relatives à la qualité médicale et à l'économie de la santé, ainsi que leur évaluation dans un but précis, mais tout en permettant une utilisation dans le cadre de problématiques diverses. » (Citation *Tour d'horizon des registres médicaux de Suisse*, FMH, 2012). Un registre de qualité met l'accent sur des indicateurs, tels que les procédures de soins, les complications ou les taux de mortalité, qui permettent une analyse de la qualité, par exemple de traitements médicaux. Un registre de dispositifs médicaux regroupe des données relatives à des dispositifs médicaux définis qui peuvent par exemple servir pour la traçabilité de l'utilisation des données, l'évaluation des risques ou la recherche.

les cas d'utilisation (y compris la nécessité de légiférer). La prise en compte globale de l'écosystème de données dans le secteur de la santé ainsi que l'aspect contextuel de la finalité et de l'appariement des données jouent un rôle important à cet égard.

Organisations participantes :

Confédération et cantons	Office fédéral de la santé publique OFSP
	Office fédéral de la statistique OFS
	Chancellerie fédérale CHf
	Office fédéral des assurances sociales OFAS
	Base logistique de l'armée (BLA) - Affaires sanitaires
	Centrale de compensation CdC
	Conférence suisse des directeurs de la santé CDS
	eHealth Suisse
Acteurs du système de santé	CARA (communauté de référence DEP)
	FMH
	GS1
	H+
	heyPatient AG (fabricant de systèmes)
	Institut de médecine sociale et préventive de l'Université de Berne
	Refdata
	Swiss Personalized Health Network (SPHN)
	SUVA
	Association Société numérique

À noter que le Préposé fédéral à la protection des données et à la transparence (PFPTD) a participé à la deuxième séance du GT CIP. Ainsi informé du travail du GT CIP, il prendra également part à l'évaluation des résultats du groupe de travail. Le PFPTD a notamment souligné que l'analyse périodique des risques selon l'article 153e LAVS jouait un rôle déterminant lors de l'utilisation du NAVS comme identificateur personnel biunivoque.

Le concept élaboré doit être soumis au GGDS à des fins d'évaluation.

3 Domaines thématiques et cas d'utilisation

Prenant pour modèle lse domaines thématiques définis pour le programme DigiSanté, les réflexions sur les identificateurs personnels se concentrent sur les quatre domaines thématiques et les cas d'utilisation suivants :

Domaine thématique	Cas d'utilisation
Processus de traitement	• **Documentation primaire** Données prélevées à des fins de documentation médicale ou des soins et données servant à la facturation. IP pour une identification biunivoque du patient. • **DEP** Échange de données pertinentes pour le traitement, dans le contexte du dossier électronique du patient. IP pour une identification biunivoque du patient et la compilation de données provenant de différentes communautés (de référence). • **Communication ciblée entre les établissements de santé** P. ex. transfert, mandat confié à un laboratoire, ordonnance. IP pour une identification biunivoque du patient.

	• **mHealth** (supporté par des applications)[3] Mesures de données vitales par des capteurs. Données saisies par le patient, p. ex. journal alimentaire ou du sommeil. IP pour l'attribution biunivoque des données saisies relatives à un patient. • **Rappel d'implants** En cas de rappel d'un implant déterminé, tous les porteurs d'implants peuvent être informés de manière ciblée. IP pour une attribution biunivoque des implants à un patient. • **Registre sur la qualité et les dispositifs médicaux**
Processus de facturation	• **Assurance sociale** (y c. AA et AI) • **Assurances complémentaires** privées proposées en complément à l'assurance-maladie sociale (voir l'art. 47*a* de la loi sur le contrat d'assurance). IP pour une attribution biunivoque des données de facturation à un patient.
Processus des autorités	• Collecte de statistiques dans le domaine de la santé selon l'ordonnance sur les relevés statistiques (RS 431.012.1) • Enregistrement des cancers selon la loi sur l'enregistrement des maladies oncologiques (RS 818.33) • Surveillance épidémiologique des maladies transmissibles selon la loi sur les épidémies (RS 818.101) • Appariement de jeux de données pour le calcul d'indicateurs de qualité médicaux selon l'art. 59*a* de la loi sur l'assurance-maladie (RS 832.10) IP pour une attribution biunivoque des données saisies relatives à une personne et appariement ultérieur des données avec des données provenant d'autres sources, notamment à des fins statistiques.
Recherche	• **Utilisation de données de sources diverses avec appariement.** IP pour une attribution biunivoque des données saisies relatives à une personne et appariement ultérieur des données avec des données provenant d'autres sources. • **Utilisation de données sans appariement**. La création d'un IP pour l'attribution biunivoque des données saisies relatives à une personne facilite le processus de gestion des données.

Le numéro AVS (NAVS) et le numéro d'identification du patient du DEP (EPR-SPID) constituent déjà deux IP biunivoques potentiels. Le NAVS peut actuellement être utilisé pour les processus de facturation des assurances sociales[4] ainsi que par les prestataires d'assurance-maladie complémentaire selon l'art. 47*a* de la loi sur le contrat d'assurance[5]. De plus, il peut être utilisé par les autorités pour l'exécution de leurs tâches ainsi que – si le droit applicable prévoit l'utilisation systématique du NAVS – par des organisations et des personnes de droit public ou privé chargées de tâches administratives par le droit fédéral, cantonal ou communal ou par contrat[6]. Une base juridique existe donc déjà pour l'utilisation du NAVS dans les domaines thématiques *Processus de facturation* et *Processus des autorités* susmentionnés. Pour le cas d'utilisation *Dossier électronique du patient* du domaine thématique *Processus de traitement*, la *loi fédérale sur le dossier électronique du patient (LDEP)* fournit une base légale spéciale pour l'utilisation de l'EPR-SPID.[7]

[3] Les réflexions sur les applications mHealth se réfèrent dans ce contexte à des applications qui sont raccordées au DEP ou à des systèmes mis à disposition par des fournisseurs de prestations. Le NAVS doit être utilisé comme IP dans les applications concernées. Aucun autre cas d'utilisation dans le contexte mHealth n'est pris en compte dans le cadre du concept. La formulation d'une recommandation pour l'utilisation d'un IP pour tous les cas d'utilisation mHealth envisageables dépasse les compétences du GT CIP dans le cadre du mandat du GGDS.

[4] Voir les art. 83 LAMAL, art. 60*a* LAA et art. 60 LAI

[5] Voir l'art. 47a LCA

[6] Voir l'art. 153c LAVS

[7] Les solutions déjà existantes pour les identificateurs personnels, comme l'EPR-SPID pour le DEP, ne doivent pas être remises en question dans ce contexte. L'objectif du présent document est de proposer des solutions pour les cas d'utilisation pour lesquels il n'existe pas encore d'IP uniforme.

L’utilisation d’un IP biunivoque reste donc à définir dans les domaines thématiques et les cas d’utilisation suivants :

- Domaine thématique *Processus de traitement* :
  - Documentation primaire/dossier médical électronique (sans référence à la facturation et hors contexte DEP)
  - Communication ciblée entre les fournisseurs de prestations
  - mHealth (supporté par des applications)
  - Registre de la qualité et de dispositifs médicaux (p. ex. pour le rappel d’implants ; géré par des organismes privés)
  - Assureurs proposant des assurances complémentaires ne tombant pas sous le coup de l’art. 47*a* LCA
  - Surveillance en temps réel des capacités hospitalières dans IES NG
- Le domaine thématique *Recherche* (en vue d’un appariement ultérieur)

Il n’existe pas à ce jour de base légale concernant l’utilisation d’un IP biunivoque, p. ex. le NAVS, comme identificateur dans le processus de traitement. C’est pourquoi on utilise actuellement dans le domaine thématique *Processus de traitement*, p. ex. pour le dossier médical, des IP locaux ou spécifiques au système. Comme mentionné plus haut, cette pratique complique la fusion des données provenant de différents systèmes et augmente le risque d’erreurs. La création d’une base légale définissant un IP biunivoque pouvant aussi être utilisé pour les données relatives aux traitements et à la recherche permettrait d’apparier ces données sans problème – sous réserve de l’obtention auprès des personnes concernées du consentement requis conformément à la législation en vigueur[8] – et fournirait à la recherche des données précieuses sur le contexte du traitement.

[8] Simplifier la procédure relative à l’octroi des consentements et à leur gestion serait judicieux. Une telle démarche de simplification permettant de donner son consentement par voie électronique a d’ailleurs été effectuée dans le cadre du projet « Espace de données pour la recherche sur la santé » et de la révision de la loi relative à la recherche sur l’être humain.

4 Options IP et évaluation

4.1 Options IP

Le GT CIP a examiné les options suivantes relatives à l'introduction d'un identificateur personnel dans le système de santé :

	Numéro AVS (NAVS)	**Numéro d'identification du patient du DEP (EPR-SPID)**	**Nouveau numéro de santé**	**Pseudonyme du numéro AVS**
Base légale	LAVS	LDEP	-	-
But d'utilisation actuel / ayants droit	• **Finalité :** exécution de tâches légales (assurance sociale, statistique de l'administration, entre autres) • **Ayants droit :** autorités, organisations et personnes habilitées selon l'art. 153*c* LAVS	• **Utilisation :** identification de patients dans le contexte du DEP • **Ayants droit :** communautés, communautés de référence et portails d'accès selon l'art. 5 LDEP	-	-
Caractéristiques / conditions-cadres	• Infrastructure et interfaces déjà mises en place pour la gestion du NAVS (système UPI de la CdC) • Les processus de consultation du numéro AVS sont standardisés (normes eCH). • Format standardisé au niveau international (EAN-13) • Un appariement direct avec les données de l'OFS est possible, car l'OFS utilise également le numéro AVS.	• Infrastructure et interfaces déjà mises en place pour la gestion de l'EPR-SPID (système UPI de la CdC) • Les processus de consultation de l'EPR-SPID sont standardisés (normes eCH). • Format standardisé au niveau international (GSRN) • Identificateur sectoriel → l'appariement avec les données d'autres secteurs est compliqué ; mais l'appariement avec le numéro AVS est possible dans UPI.	• À concevoir de A à Z (but de l'utilisation, technique, format) • L'infrastructure technique permettant de gérer le numéro doit être créée. • Ancrage légal nécessaire	• Génération de pseudonymes (spécifiques au projet) sur la base du NAVS afin d'éviter que des personnes non autorisées puissent remonter jusqu'au NAVS et apparier des données. • Nécessité de mettre en place un service de pseudonymisation • Ancrage légal nécessaire

4.2 Aperçu des arguments pour et contre l'utilisation des différents identificateurs personnels potentiels

Le tableau ci-dessous compare différents identificateurs personnels que le GT CIP envisage comme de potentiels IP.

Numéro AVS	EPR-SPID	Nouveau numéro de santé	Pseudonyme du numéro AVS
Pour : • Conformément à l'art. 153*c*, al. 1, LAVS, diverses entités sont déjà habilitées à utiliser le NAVS en dehors de l'AVS. Parmi elles figurent notamment les fournisseurs de prestations (dans le cadre des tâches qui leur sont confiées conformément à la loi fédérale sur l'assurance-maladie [LAMal]) et les services de la statistique fédérale, dont les données sont très utiles à la recherche médicale. De nouvelles bases légales relatives à une utilisation élargie du NAVS devraient toutefois être créées. • La qualité du NAVS est très élevée, et il existe de nombreuses données empiriques concernant l'utilisation du NAVS. • Une infrastructure technique centralisée est disponible (UPI). • Des normes eCH[9] ont été définies pour la gestion et l'utilisation du NAVS. • Le NAVS est déjà utilisé aujourd'hui dans le système de santé, et il est	**Pour :** • Une infrastructure technique centralisée est déjà mise en place (UP). • Des normes eCH ont été définies pour la gestion et l'utilisation de l'EPR-SPID. • Un appariement abusif avec des données provenant d'autres domaines est rendu plus difficile dans la mesure où il s'agit d'un identificateur sectoriel. Voir à ce sujet également la remarque relative au NAVS concernant l'appariement à l'aide d'autres caractéristiques se rapportant aux personnes. • Format standardisé au niveau international (GSRN) • Un numéro sectoriel répond aux exigences de la LPD concernant l'introduction du principe « privacy by design » (protection des données dès la conception). • Lorsqu'une personne change de numéro AVS (pour des raisons administratives ou après la correction d'une erreur, ce qui arrive dans 1 à 2 % des cas environ), un nouveau	**Pour :** • L'appariement abusif avec des données provenant d'autres domaines est rendu plus difficile dans la mesure où il s'agit d'un identificateur sectoriel. À ce sujet, voir également sous « Numéro AVS » la remarque concernant l'appariement au moyen d'autres caractéristiques se rapportant aux personnes. • Peut être défini selon des normes internationales. **Contre :** • L'appariement légal avec des données provenant d'autres domaines est rendu plus difficile. • Nécessité de mettre en place une nouvelle infrastructure pour la gestion des numéros de santé (coûts estimés à plusieurs dizaines de millions de francs sur une période de dix ans). • Nécessité de créer des bases légales, ce qui s'avère plus compliqué que pour les autres options IP.	**Pour :** • Remonter jusqu'à une personne en particulier au moyen du NAVS est très difficile. • L'introduction d'un nouveau numéro n'est pas nécessaire→ charges réduites au niveau législatif **Contre :** • La pseudonymisation entraîne une charge de travail supplémentaire. • Un service de pseudonymisation doit être mis en place (technique et organisation) • Un recoupement direct avec le NAVS peut être effectué en cas d'utilisation régulière, étant donné que de nombreuses institutions ont accès aussi bien au pseudonyme qu'au NAVS. • Si le nombre d'exemples est suffisant, il est possible de connaître le pseudonyme fixe en utilisant un algorithme *ad hoc.* • Lorsqu'une personne change de numéro AVS (pour des raisons administratives ou après la correction d'une erreur, ce qui arrive dans 1 à 2 % des cas environ), le nouveau

[9] L'association eCH encourage, développe et adopte des normes dans le domaine de la cyberadministration. Voir également https://www.ech.ch

Numéro AVS	EPR-SPID	Nouveau numéro de santé	Pseudonyme du numéro AVS
identifié en tant que tel par les patients. • Tout individu résidant en Suisse possède un NAVS.[10] **Contre :** • En raison de la grande diffusion du NAVS, il est théoriquement plus facile pour des personnes non autorisées d'apparier de manière illégale des données de sources diverses. Toutefois, les bases de données utilisant le NAVS sont organisées de façon décentralisée, si bien qu'il faudrait avoir accès à plusieurs de ces sources de données pour effectuer un appariement. En outre, il est fort probable que des données puissent aussi être fusionnées sans IP biunivoques, si les jeux de données comprennent d'autres données d'identification personnelle.	EPR-SPID, apparié à l'ancien, est généré. Il est donc toujours possible d'établir le lien avec la personne et son ancien numéro une fois le changement effectué. **Contre :** • L'appariement légal avec des données provenant d'autres domaines est rendu plus difficile. Un appariement avec le NAVS, par exemple, nécessiterait d'effectuer un mappage par l'intermédiaire de l'interface UPIServices. • Ancrage légal à ce jour uniquement dans la LDEP → utilisation actuellement limitée au DEP • L'EPR-SPID est peu connu du grand public. • Seuls les détenteurs d'un DEP disposent d'un tel numéro d'identification (au 15 avril 2023, 19 481 DEP avaient été créés). Avec la révision de la LDEP et la procédure d'opt out qu'elle prévoit, il faut toutefois s'attendre à une augmentation massive du nombre de DEP.	• Il faut s'attendre à des problèmes de qualité durant les premières années suivant l'introduction, car la qualité des données sources ne sera probablement pas optimale. • Le nouveau numéro de santé devrait être présenté à la population. • Tous les processus administratifs pour la gestion de ce nouveau numéro doivent être mis en place (et se chevauchent avec ceux du numéro AVS). Cela signifie que les émetteurs de l'identité primaire (registres fédéraux et cantonaux de personnes) doivent instaurer un deuxième processus de livraison des données (parallèle à celui régissant le numéro AVS) pour la nouvelle structure, ce qui va à l'encontre de la stratégie de la Confédération (p. ex. principe « once only »). • L'introduction d'un nouveau numéro de santé ne résout pas le problème des personnes ne disposant pas d'un numéro AVS (p. ex. les touristes).	pseudonyme généré n'est pas apparié avec l'ancien. On ne peut donc pas établir de lien avec la personne et son ancien numéro une fois le changement effectué. Il est possible de résoudre ce problème à l'aide d'un tableau d'appariement des pseudonymes des NAVS, ce qui implique toutefois de créer un nouveau numéro sectoriel du type EPR-SPID (au lieu d'utiliser directement cette solution).

Remarque sur la pseudonymisation des IP : la pseudonymisation du NAVS pour les cas où l'utilisation directe du NAVS est à éviter pour des raisons de protection des données revêtirait une importance majeure, notamment lors de l'utilisation du NAVS comme IP. Cela concerne par exemple le cas d'utilisation « Appariement de données pour la recherche ». Un centre de confiance (*trust center)* jouerait un rôle déterminant pour la pseudonymisation. Il pourrait notamment être chargé de

[10] De plus, un NAVS peut, si nécessaire, aussi être délivré à des personnes qui ne résident pas ou ne travaillent pas (officiellement) en Suisse, à condition que ces personnes soient en contact avec une autorité habilitée à utiliser systématiquement le NAVS. Cela concerne par exemple des sans-papiers pour lesquels l'employeur verse des cotisations sociales.

générer des pseudonymes et de les substituer aux NAVS dans les jeux de données. Ce centre assurerait en outre la gestion des clés de codage ou de décodage des pseudonymes ainsi que l’appariement des données et la mise à disposition des données appariées (voir également le chapitre 5, section *Mesures particulières pour garantir la protection des données dans le cadre de projets de recherche*).

4.3 Évaluation des options IP

Conformément à l'art. 5, let. c, LPD, les données sur la santé sont des données personnelles particulièrement sensibles. Il convient donc d'accorder une attention particulière à la protection des données lors de la décision relative à l'instauration d'un IP dans le système de santé. La simple gestion d'un IP biunivoque n'augmente que légèrement le risque pour la protection des données. Des risques surviennent dès lors que des données sensibles sont appariées à des données permettant d'identifier une personne. L'IP représente certes un moyen d'identifier une personne, mais le trio de données *nom/prénom/date de naissance* constitue lui aussi un quasi-identificateur.

Les possibilités d'appariement des données à l'aide d'un IP permettent de collecter des données ou d'établir des profils sur des personnes, ce qui représente un risque supplémentaire pour la protection des données. À noter que – comme indiqué dans les mandats du Conseil fédéral et du Parlement mentionnés au chapitre 1 – l'appariement **licite** de données de santé est une des principales motivations de l'introduction d'un IP uniforme dans le système de santé, par exemple afin de pouvoir mettre plus de données de meilleure qualité à la disposition de la recherche en matière de santé.

L'appariement de données peut toutefois aussi être réalisé à des fins malveillantes, indépendamment de l'identificateur ou du jeu d'identificateurs utilisé. Il s'agit donc d'évaluer les options IP décrites au chapitre 4 sous l'angle de la protection des données afin de déterminer laquelle offre la meilleure protection des données ou réduit la probabilité d'une fusion abusive de jeux de données par des personnes non autorisées. De plus, il est très vraisemblable que des données provenant de différents jeux de données puissent aussi être fusionnées sans utiliser un IP biunivoque, pour autant que les jeux de données concernés comprennent d'autres données permettant d'identifier une personne. Si le prénom, le nom et la date de naissance, par exemple, sont saisis sans erreur (!) dans des fichiers distincts, les données de 99,98 % de la population suisse peuvent, selon les estimations de la Conférence suisse sur l'informatique (CSI), être fusionnées de manière univoque[11].

Par rapport à l'identification au moyen d'autres caractéristiques, l'utilisation d'un IP biunivoque a aussi pour avantage d'offrir une plus grande sécurité. Lorsque des noms sont par exemple utilisés comme caractéristiques d'identification, des erreurs peuvent se produire dans le cas de noms étrangers complexes contenant des caractères spéciaux ou des lettres non latines, lors de confusions entre le nom de famille et le nom de célibataire ou dans le cas de noms phonétiquement identiques, mais ayant une orthographe différente.

Les différents IP biunivoques considérés se distinguent principalement par leur degré de diffusion actuel et par l'existence (ou l'absence) d'infrastructures techniques et organisationnelles et de bases légales.

Plus le champ d'application de l'identificateur biunivoque est limité (p. ex. au DEP ou au système de santé), moins celui-ci est utile pour les cas d'application où l'appariement de données est déterminant (p. ex. pour des projets de recherche, lorsque des données relatives au dossier médical doivent être appariées avec des données socio-économiques ou d'autres données de la statistique publique, etc.). Si un même IP est utilisé dans de nombreux jeux de données différents, la fusion de ces derniers – même par des personnes non autorisées – se trouve simplifiée dans la mesure où il suffit de connaître ce seul identificateur pour fusionner les jeux de données.

Lors de l'utilisation de différents identificateurs sectoriels, la personne qui souhaite fusionner des jeux de données doit disposer non seulement des identificateurs individuels, mais aussi d'informations sur le mappage de ces identificateurs, ce qui complique la fusion des jeux de données. Du point de vue de

[11] Voir *Le numéro AVS en tant qu'identificateur administratif univoque de la personne*, p. 4, éditeur : Conférence suisse de l'informatique

la protection des données, les identificateurs sectoriels offrent des avantages indéniables en théorie, mais très peu nombreux dans la pratique, car – comme nous l'avons déjà évoqué plus haut – il est également possible dans la plupart des cas d'apparier des données en utilisant d'autres caractéristiques d'identification. Lorsque des données sont fusionnées à des fins criminelles en particulier, on peut supposer que les auteurs de ces actes malveillants se soucient peu – pour autant que les données initiales soient de bonne qualité – qu'une infime partie des données ne puissent pas être fusionnées (0,02 % dans l'exemple précité de la CSI).

Répartir les fichiers entre des bases de données séparées est une mesure plus efficace pour empêcher une fusion de données illicite. Pour apparier des données dans une telle configuration, il faut pouvoir accéder aux différentes bases de données, ce qui complique sérieusement toute tentative d'appariement illicite. Des exigences minimales élevées en matière de sécurité des données doivent en outre être imposées aux systèmes informatiques gérant le NAVS ou tout autre IP.

Pour trancher entre utilisation du NAVS et introduction d'un nouveau numéro de santé, il faut également tenir compte, lors de l'évaluation des éventuels risques liés à la protection des données, du fait que l'utilisation du NAVS comporte le risque d'un profilage illicite de la personnalité. L'introduction d'un nouveau numéro de santé implique cependant des risques de perte de qualité (p. ex. attribution erronée d'un numéro à une personne), notamment durant la première phase d'utilisation. Il peut même en résulter des conséquences indésirables pour la santé qu'il s'agit d'éviter.

Dans ces conditions, on peut affirmer que, dans le contexte du système de santé, ce n'est pas l'IP utilisé qui constitue le facteur décisif sous l'angle de la protection des données, mais les mesures de réduction des risques mises en œuvre lors du traitement des données de santé personnelles. Ces mesures doivent se concentrer sur la protection des données de santé personnelles contre tout accès non autorisé et éventuellement de nature criminelle.

5 Conclusion et recommandation du GT CIP

Le GT CIP se prononce en faveur du NAVS comme identificateur personnel biunivoque dans les cas d'utilisation où le recoupement des données doit permettre d'établir un lien avec une personne donnée.

Cela concerne les cas d'utilisation suivants :

- Documentation primaire/dossiers médicaux électroniques (hors contexte DEP)
- Communication ciblée (p. ex. entre les fournisseurs de prestations pour les prescriptions électroniques [hors DEP] ou entre les applications mHealth et SIH, SIC ou DEP)
- Collecte de données dans le cadre de projets de recherche où un lien doit pouvoir être établi ultérieurement avec une personne, p. ex. à des fins d'appariement[12]
- Registres collectant des données personnelles sur une période prolongée
- Surveillance en temps réel des capacités hospitalières dans IES NG

Afin de permettre l'utilisation du NAVS dans les cas susmentionnés, le cercle des utilisateurs systématiques du NAVS selon l'art. 153*c* LAVS doit être élargi, dans certains cas d'utilisation, à des institutions privées (p. ex. des instituts de recherche universitaire).

Des bases légales préexistantes, une large diffusion et des infrastructures techniques déjà disponibles constituent un cadre favorable à une extension de l'utilisation du NAVS.

[12] Lorsque l'utilisation du NAVS n'est pas considérée comme nécessaire dans le cadre d'un projet de recherche, il est bien entendu aussi possible de recourir à un autre identificateur local. L'utilisation du NAVS est jugée pertinente lorsque les données doivent être appariées ultérieurement avec d'autres données ou que l'identification de la personne à laquelle se rapporte un jeu de données s'avère nécessaire (p. ex. lorsque des résultats de recherche signalent des dangers potentiels pour une personne).

Une conservation décentralisée des données est jugée nécessaire pour les fichiers utilisant le NAVS, car un tel système complique la fusion des données et offre ainsi une meilleure protection des données. Conformément aux recommandations de la CdC, les données de santé et les données personnelles doivent être traitées séparément dans les fichiers des organismes privés utilisant le NAVS.

Lors de l'utilisation du NAVS, les bases juridiques existantes doivent être strictement respectées. L'art. 153*d* *Mesures techniques et organisationnelles* et l'art. 153*e* *Analyse des risques* sont déterminants pour garantir la protection des données.

Pour les cas d'utilisation où l'établissement d'un lien avec une personne déterminée ou l'appariement de jeux de données semble peu probable, mais pas exclu, le GT CIP recommande d'utiliser un pseudonyme du NAVS spécifique au projet afin de permettre une désidentification aussi large que possible des jeux de données. Parmi ces cas figurent la plupart des projets de recherche pour lesquels des données ont déjà été préalablement appariées (p. ex. au moyen du NAVS) ou les registres qui servent à l'assurance qualité, p. ex. dans le domaine des implants (voir également les scénarios 5 et 6 au chapitre 7.1.).

S'il n'est pas forcément nécessaire de pouvoir remonter à une personne donnée ou d'effectuer un appariement avec d'autres données, n'importe quel identificateur local peut être utilisé en lieu et place du pseudonyme du NAVS.

La plupart des membres du GT CIP estiment que l'utilisation d'un IP sectoriel dans le système de santé n'est pas judicieuse pour les raisons suivantes : l'introduction d'un identificateur personnel sectoriel entraîne un bénéfice relativement faible en matière de protection des données pour des coûts relativement élevés. De plus, l'utilisation d'un pseudonyme du NAVS spécifique au projet offre un meilleur degré de protection des données qu'un IP sectoriel.

Synthèse des solutions proposées pour l'utilisation du NAVS

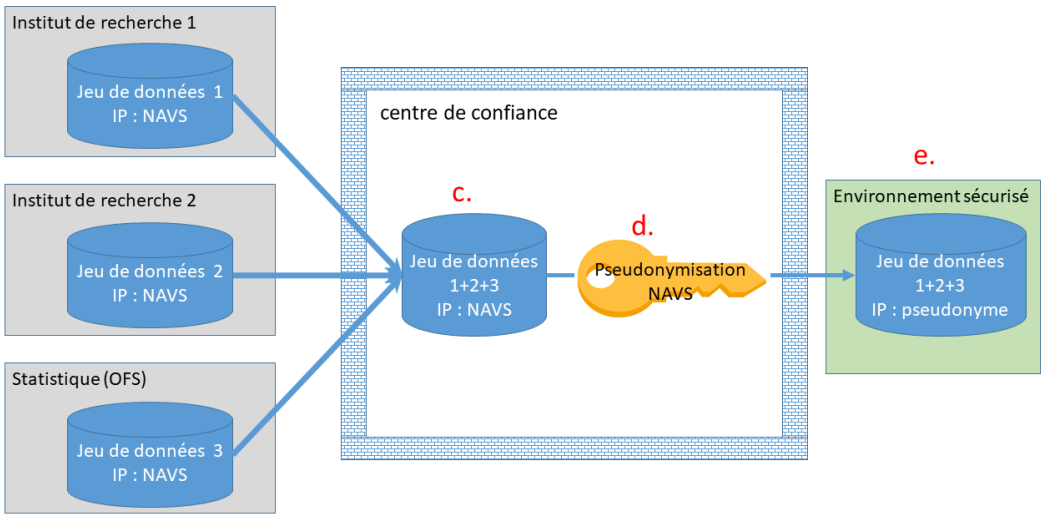
Domaine thématique	**Cas d'utilisation**	**Utilisation du NAVS**	**Une autorisation spécifique au cas est-elle requise pour utiliser le NAVS ?**
Processus de traitement	Documentation primaire/dossier médical électronique (sans référence à la facturation et hors contexte DEP)	Oui	Non
	Communication ciblée entre les fournisseurs de prestations (hors contexte DEP)	Oui	Non
	mHealth (en cas d'intégration dans les systèmes des fournisseurs de prestations)	Oui	Oui
	Registres de la qualité et de dispositifs médicaux, dans la mesure où un lien avec la personne doit pouvoir être établi (p. ex. pour le rappel d'implants ; gestion par des organismes privés ; mandat de droit fédéral existant)	Oui	Non
	Registres de la qualité et de dispositifs médicaux lorsqu'il n'est pas nécessaire de pouvoir établir un lien avec une personne	Non	-
	Prestataires d'assurances complémentaires ne tombant pas sous le coup de l'art. 47*a* LCA	Oui	Non

Recherche	Projets de recherche avec appariement de données	Oui	Oui
	Projets de recherche sans appariement de données	Non	-
	Registres sans mandat de droit fédéral	Oui	Oui

Mesures particulières pour garantir la protection des données dans le cadre de projets de recherche

Dans le contexte de la recherche et à la différence de ce qui est observé pour la plupart des autres cas d'utilisation susmentionnés, le NAVS ne sert pas prioritairement à identifier une personne pour laquelle des données sont disponibles. Dans le cadre de projets de recherche, il est généralement utilisé comme une variable d'appariement de données provenant de sources diverses. C'est pourquoi le NAVS peut le plus souvent être remplacé par un pseudonyme dans les jeux de données appariés. Lorsque le NAVS est utilisé pour apparier des données servant à des fins de recherche, il est donc nécessaire – en plus des mesures précitées et des prescriptions selon les art. 153*d* et 153*e* LAVS – de mettre en place les mesures de sécurité ci-après :

1. Les tâches suivantes doivent **être assumées par un centre de confiance** (la liste ci-dessous n'est pas exhaustive) :
    a. Évaluation des demandes des chercheurs pour l'utilisation du NAVS dans leurs jeux de données en les considérant sous l'angle de la nécessité, de la protection des données et de l'éthique
    b. Évaluation des demandes des chercheurs relatives à l'appariement de données en les considérant sous l'angle de la nécessité, de la protection des données et de l'éthique
    c. Appariement des jeux de données
    d. Remplacement du NAVS par un pseudonyme dans le jeu de données apparié. La méthode précise de pseudonymisation n'est pas définie. Toutefois, le pseudonyme doit pouvoir être relié au NAVS pour les cas où il serait nécessaire de remonter à une personne donnée ou d'effectuer ultérieurement un appariement avec d'autres jeux de données. Seul le centre de confiance a accès aux informations permettant de faire le lien entre le pseudonyme et le NAVS (voir également la let. f).
    e. Mise à disposition des jeux de données appariés en vue de leur traitement par les chercheurs dans un environnement sécurisé



f. Archivage sécurisé des jeux de données appariés et informations sur le mappage, une fois les données traitées par les chercheurs.[13]
g. Garantir que les données appariées soient accessibles uniquement aux chercheurs et aux collaborateurs responsables au sein du centre de confiance.
h. Informer les contributeurs de données, c.-à-d. les personnes dont les données sont utilisées, de l'utilisation de leurs données.

2. Les conditions suivantes qui régissent l'utilisation du NAVS dans des projets de recherche doivent être ancrées dans la loi :

   a. Toute utilisation du NAVS dans un projet de recherche nécessite une autorisation du centre de confiance et/ou de la commission d'éthique compétente. Il convient à cet égard de respecter les dispositions légales en vigueur. D'autres bases légales seront définies si nécessaire.
   b. L'appariement de données à des fins de recherche à l'aide du NAVS requiert l'autorisation du centre de confiance.

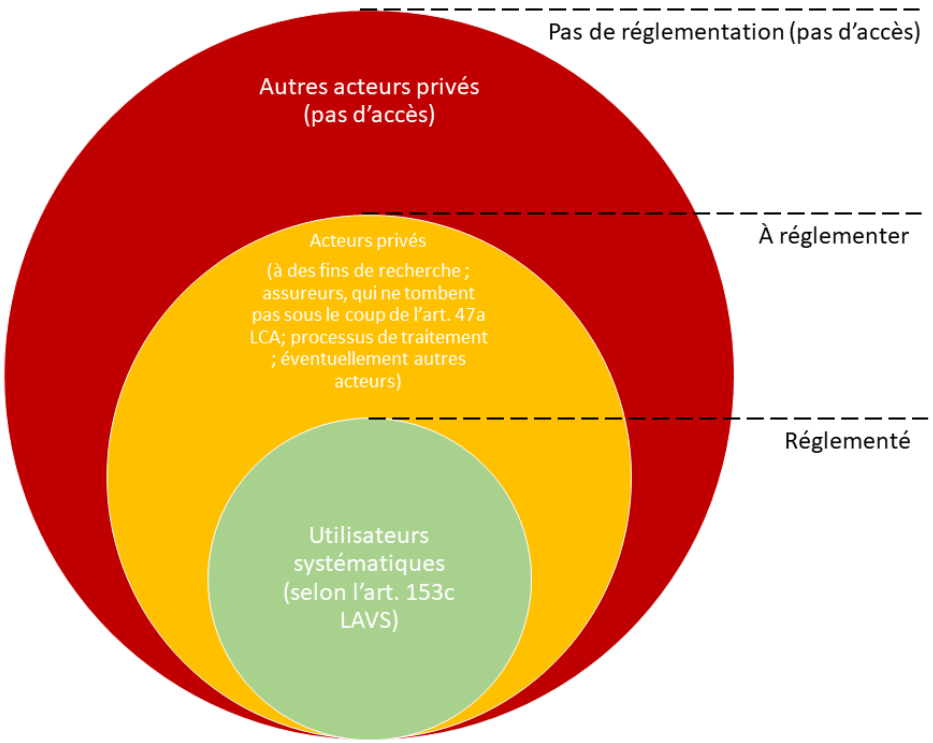
3. Seul le centre de confiance est habilité à apparier des jeux de données.

4. Les chercheurs ne sont pas autorisés à intégrer les données provenant des jeux de données appariés dans leurs propres fichiers de données.

6 Remarque sur le besoin de légiférer

Le GGDS ne déterminera fermement le besoin de légiférer qu'une fois le concept validé.

Les utilisations actuelles et le domaine à réglementer sont représentés schématiquement dans le graphique ci-dessous.



[13] Conformément au *Code d'intégrité scientifique des Académies suisses des sciences,* l'archivage des données permet d'assurer que les données soient reproductibles et/ou vérifiables (en fonction de la discipline), fiables et exactes (voir le *Code d'intégrité scientifique,* chapitre 4.5). Par ailleurs, il semble également judicieux de conserver des données qui ont été appariées pour des projets de recherche qui seraient menés ultérieurement et se référaient à ces mêmes données, dans le but de réduire la charge de travail liée à l'appariement.

Dans le sillage des discussions menées au sein du GT CIP, le besoin de légiférer suivant a été identifié :

- Le cercle des utilisateurs systématiques du NAVS hors AVS (art. 153*c* LAVS) doit être élargi. Cela concerne par exemple les institutions qui traitent des données à des fins de recherche, les fournisseurs de prestations qui gèrent la documentation primaire, les institutions qui, chargées par le droit fédéral, tiennent des registres de qualité à l'échelle nationale, ou encore les prestataires qui proposent des assurances-maladie complémentaires ne tombant pas sous le coup de l'art. 47*a* LCA.
- Ancrage légal de l'autorisation d'utiliser le NAVS dans des jeux de données dans le contexte de la recherche (en matière de santé), y c. pour les registres qui ne sont pas tenus par mandat de droit fédéral. L'autorisation d'utiliser le NAVS dans le cadre de projets de recherche doit être délivrée au cas par cas par un centre de confiance ou une commission d'éthique.
- Tout centre de confiance assumant les tâches définies au chapitre 5 doit être ancré dans la loi.
- Seul un centre de confiance est habilité à apparier des données à des fins de recherche.
- Si cela s'avère nécessaire pour un cas d'utilisation, l'utilisation du NAVS par des organisations et des personnes de droit public ou de droit privé visées à l'art. 153*c*, al. 1, let. a, ch. 4, LAVS doit être ancrée dans des dispositions légales spécifiques correspondantes.
- Ancrage légal des exigences posées aux applications mHealth qui souhaitent utiliser le NAVS.

7 Annexe

7.1 Annexe 1 : scénarios relatifs à l'utilisation du NAVS / pseudonyme

7.1.1 Scénario 1 : documentation primaire / gestion de données dans le dossier médical électronique

Un professionnel de la santé (PS) documente des données médicales, telles que l'anamnèse, les diagnostics, les résultats d'examens, les radiographies, les médications, etc. dans le dossier médical électronique d'un patient. Si un traitement ultérieur est nécessaire, le PS doit être en mesure d'attribuer directement les données à la personne concernée et d'identifier celle-ci. Dans ce cas, le NAVS doit être utilisé comme un identificateur personnel permettant d'identifier de manière biunivoque la personne en question.

7.1.2 Scénario 2 : communication ciblée entre les fournisseurs de prestations

Le PS A transfère la patiente M au PS B. Ce dernier doit être en mesure d'attribuer clairement à une personne ce transfert ainsi que les documents et données médicales fournis afin de pouvoir convoquer la bonne personne et poursuivre ainsi le traitement. Dans ce cas, le NAVS doit être utilisé comme un identificateur personnel biunivoque pour la personne en question.

7.1.3 Scénario 3 : projet de recherche avec attribution des données de recherche à une personne

Des analyses doivent être réalisées dans le cadre d'un projet de recherche, et il est fort probable que les résultats de ces analyses révèlent des risques de santé potentiellement graves pour les personnes concernées. Dans ce cas, la personne concernée doit pouvoir être informée de ces risques afin que des mesures correspondantes puissent être prises pour éviter tout risque d'atteinte à sa santé. Ici, le NAVS doit être utilisé comme un IP permettant d'identifier la personne concernée de manière biunivoque.

7.1.4 Scénario 4 : projet de recherche pour lequel des données de sources diverses doivent être appariées

Des données personnelles sont collectées dans le cadre d'un projet de recherche. Ce n'est qu'après appariement avec des données d'autres sources qu'elles sont pertinentes ou gagnent en pertinence. L'appariement des données nécessite un IP uniforme pour l'ensemble des fichiers de données concernés. Dans ce cas, le NAVS doit être traité comme un IP, étant donné qu'il est déjà utilisé en tant qu'IP

pour de nombreux fichiers de données et que les infrastructures permettant l'utilisation du NAVS sont disponibles.

Dans le jeu de données apparié, le NAVS est remplacé par un pseudonyme qui pourra être à nouveau relié à ce numéro s'il était nécessaire de remonter à une personne donnée ou d'effectuer ultérieurement un appariement avec d'autres données.

7.1.5 Scénario 5 : projets de recherche utilisant des données qui ne doivent pas renvoyer à une personne à identifier

Dans le cadre d'un projet de recherche, les données utilisées doivent pouvoir être attribuées de manière univoque à une personne (individualisation du jeu de données). La personne en question ne doit toutefois pas être connue pour le but de la recherche (personnalisation du jeu de données). Dans ce cas, il convient d'utiliser un pseudonyme du NAVS ou tout autre identificateur local afin de pouvoir attribuer les données de manière univoque à un individu. Lors de l'utilisation d'un pseudonyme du NAVS, la personne à laquelle correspond effectivement le pseudonyme ne peut être identifiée qu'au moyen d'une clé gérée par une tierce partie de confiance.

7.1.6 Scénario 6 : registre des implants

Le registre des implants consigne des informations qui indiquent quelle personne a reçu quel implant. En général, le porteur d'un implant n'a pas besoin d'être identifié. En cas de défaut du produit, ou lorsque des risques liés à un implant ne sont constatés qu'a posteriori, il peut toutefois être nécessaire d'informer les personnes en question des risques encourus ou du remplacement éventuel de leur dispositif. Dans ce cas, un pseudonyme du NAVS doit être utilisé afin de pouvoir attribuer de manière univoque les données figurant dans le registre des implants à la personne concernée. Si nécessaire, la personne à laquelle correspond effectivement le pseudonyme peut être identifiée au moyen d'une clé gérée par une tierce partie de confiance.

7.2 Annexe 2 : prises de position sur les déclarations contenues dans le document

7.2.1 Prise de position de la FMH

La FMH remercie l'OFSP de lui avoir offert la possibilité de prendre position sur le concept d'identificateur de personnes, position qui diverge de celle du GT CIP.

Pour des raisons liées à la protection des données, la FMH se prononce en faveur d'un IP sectoriel, car cette solution renforce notamment le principe de finalité et garantit que les données seront confinées au contexte sanitaire. L'EPR-SPID constitue déjà un IP sectoriel, utilisé dans le domaine de la santé. L'introduction d'un nouveau numéro de santé n'est pas nécessaire et l'utilisation du numéro AVS comme identificateur de patient universel entraînerait des risques supplémentaires.

Le principal risque lié à l'utilisation du NAVS comme IP ne concerne pas l'interconnexion de bases de données. Utilisé à large échelle, le NAVS ne serait plus en effet un identificateur « non parlant », mais une donnée personnelle susceptible d'être attribuée facilement à une personne identifiée ou identifiable. Le NAVS est mentionné avec le nom de famille complet sur les documents publics (p. ex. sur la carte d'assuré). De plus, le risque est élevé que des données sanitaires puissent être recoupées avec des données personnelles provenant d'autres domaines (p. ex. données fiscales, données du casier judiciaire) (message LDEP 2013, p. 4784).

En outre, la recherche médicale n'a pas besoin de données personnelles (NAVS), mais de données individualisées. Selon la FMH, la transmission de données personnelles à des fins de recherche requiert un consentement, à la différence de la transmission de données individualisées non personnelles. L'utilisation du NAVS comme identificateur de personne est donc inappropriée et complique la communication de données (voir également le projet de consultation pour la révision de la LDEP, art. 19f et 19*g*).

L'utilité pour les cas d'utilisation mentionnés dans le concept est la même quel que soit l'IP choisi. Les mesures techniques et organisationnelles visant à garantir la sécurité des données sont toutefois différentes. L'affirmation selon laquelle ce n'est pas l'IP utilisé qui, dans le contexte du système de santé, constitue le facteur décisif au regard de la protection des données n'est pas exacte. Du point de vue de la protection des données, en vertu de l'art. 7, al. 1 LPD, il est impératif de choisir une solution technique qui garantisse en particulier les principes fixés à l'art. 6 LPD (entre autres, le principe de finalité). Seul un IP sectoriel remplit ces conditions.

Position / conclusion de la FMH

La FMH ne juge pas convaincants les arguments en faveur du NAVS qui sont énumérés dans le concept. Elle considère que nombre des arguments présentés en ce sens valent aussi pour un IP sectoriel comme l'EPR-SPID ou, pour le moins, parlent en sa faveur. Du point de vue de la FMH, le choix doit clairement se porter sur l'EPR-SPID, qui a été conçu comme un IP sectoriel pour le domaine de la santé et qui, conformément au projet de consultation pour la révision de la LDEP, doit être diffusé au sein du système de santé, grâce notamment à des interfaces pour l'utilisation des données dans la recherche. La FMH rejette par conséquent l'utilisation du NAVS comme identificateur de patient universel.

7.2.2 Prise de position de la Société numérique

La Société numérique remercie l'OFSP de lui avoir offert la possibilité de prendre position sur le concept d'identificateur de personne, position qui diverge de celle du GT CIP.

Cette organisation à but non lucratif s'investit pour la protection des citoyens, représente les intérêts de la société civile et s'engage en faveur de la protection des données ainsi que de la défense des droits humains et fondamentaux dans l'espace numérique.

Dans cette optique, la Société numérique partage les réserves en matière de protection des données de la FMH concernant le concept d'identificateur de personne dans le système de santé et s'oppose donc à l'utilisation du NAVS comme identificateur de personne.

Elle demande que l'autodétermination informationnelle soit également garantie pour les identificateurs de personnes utilisés dans le système de santé, avec des prescriptions portant sur les points suivants :

- établissement d'un procès-verbal des accès à des données de santé personnelles et définition de la durée de conservation des procès-verbaux ;
- droit à l'information selon la législation sur la protection des données, y compris pour les accès à des données de santé personnelles ;
- obligation de déclarer et application systématique du droit en cas d'utilisation abusive (p. ex. du NAVS).

Propositions spécifiques

- Le concept propose comme seule solution un IP (« universel »), utilisé dans de larges domaines, qui doit permettre, pour les cas d'utilisation décrits, d'identifier des objets et des personnes de manière univoque, tous systèmes confondus. L'utilisation de divers identificateurs sectoriels (selon des normes telles que l'IHE) est certes jugée utile sous l'angle de la protection des données, mais considérée comme trop compliquée. À cet égard, on peine à comprendre pourquoi les normes qui sont adoptées par les fabricants et les utilisateurs à l'échelle internationale en matière de structures de données et d'interfaces seraient « trop compliquées » pour les systèmes disponibles sur le marché pour le traitement de données sanitaires.
- Selon les termes du concept, un « IP supplémentaire » tel que le NAVS représenterait un « risque pour la protection des données seulement légèrement accru » pour les données

de santé personnelles. De manière un peu paradoxale, « conformément aux recommandations de la CdC, les données de santé et les données personnelles doivent être traitées séparément dans les fichiers des organismes privés utilisant le NAVS. »

=> Dans ce contexte, les termes « doivent » et « recommandations » sont clairement trop peu contraignants et vont également à l'encontre de l'argument selon lequel « d'autres données d'identification personnelles sont déjà disponibles. » On peut citer, par exemple, les cas d'utilisation d'« identification implicite » liés à la saisie de données individualisées à l'aide d'applications mHealth installées sur des appareils connectés personnels (« smart devices »): du fait de ces trop faibles contraintes, tous les identificateurs d'un appareil connecté pourraient être fusionnés avec le NAVS. Dès lors, on ne voit pas comment une utilisation à des fins abusives, comme le profilage, pourrait être détectée et empêchée de manière efficace.

C'est pourquoi les données non médicales qui permettent d'identifier une personne et les données de santé **doivent impérativement** être enregistrées séparément. Elles peuvent être fusionnées dans un but précis, notamment à des fins de traitement en cas d'utilisation concrète au sein d'un environnement sécurisé de manière adaptée (p. ex. dans les systèmes informatiques hospitaliers ou les systèmes informatiques de cabinets médicaux). Dans le contexte de l'« identification de patients », les normes IHE fournissent des exemples éprouvés concernant l'étendue et la nature d'utilisations concrètes.

- Le présent concept veut mettre l'accent sur des cas d'utilisation pour lesquels il n'existe pas encore d'IP univoque. Selon l'approche proposée, le NAVS doit être utilisé pour une (auto-)identification univoque du patient en contact direct avec le fournisseur de prestations. Dans le même temps, son utilisation doit être autorisée dans la documentation primaire dans le contexte de « traitements médicaux sans référence à la facturation et hors contexte DEP ».

En raison des travaux en cours sur une nouvelle version du DEP et de la révision de la LDEP (en consultation), l'étendue, l'interface et le fonctionnement du futur « contexte DEP» n'ont pas encore été déterminés de manière définitive. La notion de « moyens d'identification » (art. 7 AP-LDEP) englobe au moins une future version d'un e-ID pour l'identification des patients et l'accès au DEP.
Le nombre de « traitements médicaux sans référence à la facturation et hors contexte DEP » devrait donc être négligeable en cas d'introduction réussie d'un DEP. L'utilité de l'extension proposée du NAVS à d'autres applications spéciales (p. ex. la communication entre l'ordonnance électronique, les applis mHealth, le SIH, le SIC ou le DEP), qui dépendent également de la conception définitive du futur DEP, reste discutable.

Pour les applications mHealth en particulier, le présent concept admet la nécessité d'une autorisation spécifique pour l'utilisation du NAVS sans fournir pour autant une description des critères sous-tendant cette autorisation, comme l'efficacité médicale ou les applications alternatives (génériques). La saisie de données biologiques, par exemple, par le biais de capteurs et d'applications avec une intégration dans les systèmes des fournisseurs de prestations conformément à l'état actuel de la technique génère d'autres métadonnées avec une identification implicite (voir ci-dessus). L'application systématique d'IP sectoriels rend transparentes la fusion et l'évaluation systématique des données par des tiers autorisés ou non, et autorise alors une autodétermination informationnelle pour les patients.

Conclusion et recommandation

Le concept d'« identificateurs de personnes dans le système de santé » devrait tenir compte des exigences fondamentales susmentionnées, et son contenu devrait être élaboré parallèlement au développement continu du dossier électronique du patient (DEP), dans le but de créer un système global composé de modules harmonisés selon les principes de protection des données du « *privacy by design* ».