Commission nationale de l'informatique et des libertés

Délibération n° 2023-081 du 20 juillet 2023 portant avis sur un projet d'arrêté relatif au référentiel de sécurité applicable au Système national des données de santé

NOR : *CNIX2412723X*

N° de demande d'avis : 23001213.	**Textes concernés :** projet d'arrêté relatif au référentiel de sécurité applicable au Système national des données de santé.
Thématiques : Système national de données de santé (SNDS), sécurité des systèmes d'information.	**Fondement de la saisine :** article 8.I.4°-*a* de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et articles L. 1461-1 et R. 1461-6 du code de la santé publique.

L'essentiel :

Le projet d'arrêté vise à mettre à jour les exigences de sécurité applicables aux systèmes d'information et traitements utilisant des données à caractère personnel issues du SNDS.

La CNIL salue l'ambition de sécuriser l'ensemble des systèmes d'information comprenant des données du SNDS, mais préconise que le périmètre d'application du référentiel soit clarifié.

Compte tenu du niveau particulièrement élevé des exigences qu'il contient ainsi que des possibles freins au partage des données qu'il risque de générer, elle invite le ministère à fournir aux acteurs concernés des moyens humains et financiers suffisants afin de leur permettre de se mettre en conformité.

La Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (loi « informatique et libertés ») ;

Vu la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé ;

Vu l'arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé ;

Vu la délibération n° 2017-022 du 26 janvier 2017 portant avis sur un projet de décret relatif au référentiel de sécurité applicable au Système national des données de santé ;

Après avoir entendu le rapport de Mme Valérie PEUGEOT, commissaire, et les observations de M. Damien MILIC, commissaire du Gouvernement,

Adopte la délibération suivante :

I. – **La saisine**

A. – *Le contexte*

Le Système national des données de santé (SNDS), créé par la loi n° 2016-41 du 26 janvier 2016, a pour finalité la mise disposition de données à caractère personnel concernant la santé, afin notamment de mettre en œuvre des traitements à des fins de recherches, d'études ou d'évaluations dans le domaine de la santé répondant à un motif d'intérêt public.

Initialement circonscrit au « SNDS historique », c'est-à-dire aux données issues des bases médico-administratives hébergées ou susceptibles d'être hébergées par la Caisse nationale de l'assurance maladie (CNAM), le périmètre des catégories de données le composant a été élargi par la loi n° 2019-774 du 24 juillet 2019 (données issues de la prise en charge médicale, des visites médicales scolaires, des services de protection maternelle ou infantile, des visites de santé au travail ou des enquêtes appariées, etc.).

Lorsqu'elles sont traitées pour l'une des finalités mentionnées au III de l'article L. 1461-1 du code de la santé publique (CSP), les catégories de données visées au I de l'article L. 1461-1 du CSP composent le SNDS « élargi » (ou « données du SNDS »). Elles sont alors soumises à l'ensemble des dispositions de ce code. En particulier, les gestionnaires des bases de données du SNDS doivent respecter le référentiel de sécurité, ne poursuivre aucune finalité interdite, respecter les conditions d'accès aux données via un accès permanent ou à la réalisation d'une formalité, se conformer aux modalités de transparence. Une partie de ces données a alors vocation à être intégrée progressivement dans un « SNDS central » géré par la CNAM et par la Plateforme des données de santé (PDS). Ce « SNDS central » est composé d'une base principale (comprenant à ce jour le « SNDS historique » ainsi que

d'autres bases couvrant l'ensemble de la population bases telles que « SI-DEP » et « Vaccin-COVID ») et d'un catalogue incluant d'autres bases de données.

Afin de garantir un niveau de sécurité suffisant, l'accès aux données du SNDS doit s'effectuer dans des conditions assurant la confidentialité, l'intégrité des données et la traçabilité des accès et des autres traitements, conformément à un référentiel défini par l'arrêté, tel que prévu au 3 du IV de l'article L. 1461-1 et à l'article R. 1461-7 du CSP (« référentiel de sécurité du SNDS »).

B. – *L'objet de la saisine*

Le projet d'arrêté a pour objet la mise à jour du précédent référentiel de sécurité du SNDS issu de l'arrêté du 22 mars 2017 en raison des évolutions du cadre juridique et de l'état de l'art en matière de sécurité des données.

Le projet de référentiel définit les exigences de sécurité que doivent mettre en œuvre les responsables de traitement et les gestionnaires des différents systèmes d'information traitant des données du SNDS, sur la base :

– de principes généraux, déclinés de façon opérationnelle au moyen d'une analyse de risques ;
– de la prise de mesures techniques et organisationnelles afin de réduire ces risques ;
– d'une homologation avec acceptation des risques résiduels.

II. – **L'avis de la CNIL**

A. – *Concernant le périmètre d'application du référentiel de sécurité applicable au SNDS*

La CNIL relève que l'élargissement du périmètre des données du SNDS opéré en 2019 a pour conséquence d'accroître celui du référentiel de sécurité du SNDS qui prévoit désormais quatre cas d'usage. Le ministère a explicité ces cas en les illustrant avec des exemples dont certains sont repris ci-dessous.

Ainsi, selon les éléments transmis par le ministère, le champ d'application du projet de référentiel s'étend aux systèmes rassemblant et assurant la mise à disposition des données du SNDS pour les finalités du SNDS (appelés « système du SNDS ») pouvant impliquer :

– soit une « **mise à disposition** » des données via un « espace projet » ;
– soit une « **transmission des données** », c'est-à-dire l'envoi des données à un « autre système du SNDS ».

Ces différentes notions sont définies dans le projet de référentiel. Le ministère a précisé que le référentiel s'appliquera dès lors qu'interviendra une transmission ou une mise à disposition des données du SNDS à un autre responsable de traitement, que celui-ci soit un responsable de traitement conjoint ou responsable d'un traitement ultérieur. A cet égard, le ministère s'est engagé à modifier la définition de « mise à disposition » afin de préciser qu'« un traitement de données mis en œuvre dans le cadre d'une co-responsabilité entre le responsable de traitement du système d'information et un tiers » constitue une « mise à disposition ».

Par ailleurs, d'une manière générale, selon les précisions apportées par le ministère, le projet de référentiel :

– ne s'appliquera pas lorsque les données du SNDS sont utilisées par le gestionnaire du système du SNDS pour ses propres traitements ;
– s'appliquera uniquement lors de la mise à disposition et de la transmission des données issues des « bases sources » telles que les entrepôts hospitaliers, et non à l'hébergement des données.

Ces précisions faites, le projet de référentiel prévoit les quatre cas d'usage décrits ci-après.

Le premier cas d'usage est relatif au « SNDS central ». Le projet reprend ce cas déjà prévu dans le précédent référentiel tout en précisant qu'il sera également applicable à l'alimentation, l'hébergement et la transmission, y compris entre les gestionnaires de système du « SNDS central ».

Le deuxième cas d'usage porte sur l'application du référentiel aux « systèmes fils » pour l'hébergement, la transmission et la mise à disposition des données du SNDS. Sont définis comme « systèmes fils » l'ensemble des systèmes du SNDS rassemblant ou mettant à disposition des données du SNDS dans le cadre des finalités du SNDS, transmises soit par le SNDS central, soit par un autre système fils ou encore par un autre système du SNDS. Le ministère estime donc que le référentiel sera notamment applicable à un entrepôt de données de santé qui rassemble et permet la mise à disposition à des tiers de données provenant des dossiers médicaux des patients, et ce à des fins de recherche. Dans le silence du projet de référentiel, s'agissant des entrepôts de données de santé alimentant la base catalogue du SNDS et conservés par leur responsable de traitement initial en vue d'une mise à disposition ou d'une transmission de données à des tiers pour des finalités SNDS, la CNIL en déduit que leur hébergement devra être réalisé en conformité avec le référentiel de sécurité du SNDS.

Le troisième cas d'usage concerne les bases de données qui alimentent le « SNDS central » ou un « autre système du SNDS ». Dans cette hypothèse, le référentiel s'applique uniquement :

– lors de la mise à disposition à un tiers pour des finalités du SNDS ;
– lors de la transmission de données vers un « système SNDS ».

Le dernier cas d'usage concerne les « systèmes du SNDS n'alimentant ni le SNDS central, ni un système fils, ni un autre système du SNDS ». Le référentiel s'applique alors uniquement :

– à la mise à disposition de données du SNDS à un tiers pour des finalités du SNDS : par exemple, lorsque des données d'une cohorte constituée de données issues de l'administration de questionnaires combinées à des données recueillies dans le cadre du soin sont mises à disposition d'un tiers à des fins de recherche ;
– à la transmission de données du SNDS vers un « autre système du SNDS » : par exemple, un établissement transmettant des données issues de dossiers médicaux à un autre établissement de santé en vue d'une recherche multicentrique.

S'agissant de la notion d'« autre système du SNDS », le ministère a précisé qu'il s'agissait d'une « base de données contenant des données du SNDS et non qualifiée de système fils ». Il s'est engagé à inclure cette définition dans le référentiel.

La CNIL prend également acte de ce que, selon le ministère, le référentiel sera également applicable, dans le cadre du dernier cas d'usage, à une transmission de données du SNDS à un tiers, que les données soient ou non versées dans « un autre système du SNDS ».

La CNIL salue l'ambition du ministère de sécuriser l'ensemble des traitements mettant à disposition des données du SNDS à un tiers pour l'une des finalités du SNDS.

Elle relève cependant que son application apparait particulièrement complexe à mettre en œuvre, notamment pour ce qui concerne les deux derniers cas d'usage. En effet, le projet de référentiel s'appliquera à la seule mise à disposition ou à la seule transmission des données pour des finalités du SNDS, mais ne s'appliquera pas au simple hébergement des données. Elle estime que le référentiel sera particulièrement délicat à mettre en œuvre, notamment pour les projets en cours qui se prolongeront au-delà des deux ans de la période transitoire prévue par le projet d'arrêté, et pour lesquels les données ont déjà été transmises par le gestionnaire du système.

Elle s'inquiète par ailleurs d'un référentiel de sécurité qui resterait partiellement lettre morte, en raison du manque de compétences techniques et de moyens de certains acteurs de la recherche. Cela aurait alors pour conséquence de décourager les organismes disposant de moindres moyens de partager les données à des fins de recherches en santé.

En tout état de cause, elle estime que le périmètre d'application du référentiel devrait être énoncé de façon plus détaillée afin d'améliorer la clarté du dispositif. A cet égard, elle prend acte de l'engagement du ministère d'intégrer des exemples précis dans la documentation pédagogique qui accompagnera la publication de ce référentiel.

Par ailleurs, la CNIL appelle le ministère à fournir aux acteurs de la recherche et à l'écosystème les moyens nécessaires afin qu'ils puissent mettre en conformité, vis-à-vis des exigences de sécurité du projet de référentiel, les outils leur permettant d'effectuer leurs études.

B. – *Concernant les dispositions transitoires de l'arrêté*

Le projet d'arrêté prévoit une application progressive du référentiel de sécurité :

– les systèmes du SNDS existants soumis au précédent référentiel devront être en conformité totale avec le référentiel mis à jour pour leur prochaine homologation de sécurité et au plus tard dans un délai de deux ans à compter de sa publication ;
– les systèmes du SNDS existants mais non soumis au précédent référentiel devront être en conformité avec le référentiel mis à jour dans un délai de deux ans à compter de sa publication ;
– les systèmes d'information créés après l'entrée en vigueur de l'arrêté devront être en conformité avec le référentiel mis à jour dès leur création.

Tous les systèmes du SNDS existants devront, en outre, établir un plan d'action de mise en conformité avec le référentiel mis à jour, dans un délai de six mois à compter de sa publication.

Le ministère a précisé privilégier la mise en conformité directement avec le nouveau référentiel, pour les systèmes du SNDS existants mais non soumis au précédent référentiel. Selon lui, l'encadrement actuel de ces systèmes (le précédent référentiel, mais aussi le référentiel relatif aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données dans le domaine de la santé, etc.) impose un niveau de sécurité et de confidentialité comparable à celui prévu par le projet de référentiel.

La CNIL s'interroge sur la variabilité des niveaux de sécurité des systèmes SNDS entrant dans le champ d'application du projet de référentiel pendant la période transitoire. En effet, parmi les systèmes qui devront respecter le nouveau référentiel, certains ne sont soumis ni au précédent référentiel ni à celui applicable aux entrepôts de données de santé. Il en résulte des risques en matière de sécurité pendant la période transitoire. La CNIL invite donc le ministère à préciser dans le projet de référentiel que le plan d'action de mise en conformité devra prévoir une priorisation des mesures en fonction des risques identifiés.

C. – *S'agissant des mesures de sécurité que doivent mettre en œuvre les « systèmes du SNDS »*

S'agissant des exigences générales en matière de sécurité :

En premier lieu, le précédent référentiel indiquait que les systèmes du SNDS devaient s'assurer du respect des règles « *de la Politique générale de sécurité des systèmes d'information en santé (PGSSI-S), de la Politique de*

sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS), des règles applicables dans le cadre du Référentiel Général de Sécurité (RGS) ». Ces mentions ne figurent plus dans le projet de référentiel.

Le ministère a indiqué que la PGSSI-S et le RGS n'avaient pas vocation à s'appliquer à l'environnement informatique des systèmes du SNDS. Il s'est néanmoins engagé à rétablir la référence à la PSSI-MCAS et à mentionner le décret nº 2022-513 du 8 avril 2022, qui encadrent chacun les règles de sécurité des systèmes d'information de l'Etat, considérant que les systèmes du SNDS constituent des infrastructures informatiques entrant dans leurs champs d'application. **Pour ces mêmes raisons, la CNIL invite le ministère à s'interroger sur l'applicabilité de la circulaire nº 6404/SG du 31 mai 2023 portant actualisation de la doctrine d'utilisation de l'informatique en nuage par l'Etat aux systèmes du SNDS.**

En second lieu, le projet de référentiel prévoit que l'homologation de sécurité sera désormais à la charge du gestionnaire du système du SNDS y compris « *dans le cadre de la mise à disposition dans des espaces projets par le gestionnaire du système* ». La CNIL salue cette évolution qui correspond davantage à la réalité dans la mesure où les systèmes fils ne sont pas toujours mis en œuvre par les responsables de traitements, mais également par des prestataires spécialisés regroupant et hébergeant un grand nombre d'entre eux.

Afin d'assurer la transparence et la visibilité sur l'ensemble des systèmes homologués pour traiter des données du SNDS, la CNIL prend acte de l'intention du ministère d'engager des travaux dans la perspective de la création d'un annuaire ou d'un répertoire public. Néanmoins, afin de ne pas priver d'effectivité l'ensemble du dispositif d'homologation et de conformité au référentiel de sécurité, elle estime que ce nouvel outil devrait être renseigné de façon systématique par les gestionnaires de ces systèmes.

La CNIL prend acte de l'engagement du ministère de modifier le projet de référentiel afin de mettre à la charge du gestionnaire du système du SNDS l'obligation de s'assurer que les conditions légales sont réunies avant d'ouvrir l'accès aux données aux personnes physiques accédant à des données d'un système du SNDS dans un espace projet sous la responsabilité d'un responsable de traitement (les « utilisateurs ») comme aux administrateurs fonctionnels et techniques du système du SNDS (les « administrateurs »).

S'agissant de la territorialité des données du SNDS :

Le référentiel rappelle le principe prévu par les dispositions de l'article R. 1461-1 du CSP selon lequel les données du SNDS sont hébergées au sein de l'Union européenne. Par ailleurs, aucun transfert de données à caractère personnel ne peut être réalisé, sauf dans le cas d'accès ponctuels pour une finalité relevant du 1º du I de l'article L. 1461-3.

La CNIL rappelle que cette exclusion des transferts en dehors de l'Union européenne ne suffit cependant pas à écarter les risques d'accès par un tiers non autorisé aux données du SNDS hébergées par des prestataires non soumis exclusivement aux lois de l'Union européenne.

La CNIL prend acte de l'engagement du ministère de compléter le projet de référentiel sur les exigences auxquelles les gestionnaires des systèmes du SNDS devront se soumettre pour réduire substantiellement ces risques d'accès. En particulier, les gestionnaires ou les sous-traitants susceptibles d'être soumis à la législation d'un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 45 du RGPD, auront pour obligation d'identifier les législations en cause, de mettre en œuvre des mesures pour atténuer les risques d'accès non autorisé induits par ces réglementations et d'identifier les risques résiduels qui demeureraient malgré ces mesures.

Toutefois, au regard de la sensibilité et du volume des données figurant dans la base principale du SNDS, la CNIL estime que les organismes rassemblant et mettant à disposition ces données pour des finalités SNDS ainsi que leurs sous-traitants doivent être exclusivement soumis aux lois de l'Union européenne.

S'agissant des mesures de sécurité applicables en cas d'accès aux données du SNDS :

Le projet de référentiel prévoit qu'en cas d'urgence les gestionnaires des systèmes peuvent suspendre temporairement l'accès au SNDS.

La CNIL relève que le ministère souhaite modifier ce paragraphe afin d'indiquer que seuls les responsables des traitements mentionnés au II de l'article L. 1461-1 du CSP, c'est-à-dire la CNAM et la Plateforme de données de santé, « *peuvent suspendre temporairement l'accès aux données du Système national des données de santé* » conformément aux dispositions de l'article 77 de la loi « informatique et libertés ».

La CNIL prend acte de l'engagement du ministère :

– de prévoir une suspension temporaire de l'accès par les gestionnaires à tout système du SNDS en cas d'incident grave, en informant immédiatement le ou les responsables de traitements ;
– de rappeler le principe d'une notification aux autorités compétentes en cas de violation de données susceptible d'engendrer un risque pour les droits et libertés des personnes concernées ;
– de réintroduire dans le référentiel le principe selon lequel les administrateurs ne devront pas avoir accès à Internet depuis les environnements d'administration du SNDS élargi.

S'agissant des mesures de pseudonymisation des données :

La CNIL prend acte de l'engagement du ministère de compléter le référentiel afin qu'il prévoie le renouvellement des pseudonymes en cas de compromission avérée de la fonction de pseudonymisation utilisée. La

CNIL recommande néanmoins que dans le cas où une vulnérabilité est constatée, la fonction de pseudonymisation soit modifiée.

En outre, différents usages de la pseudonymisation sont prévus. En particulier, il est mentionné à plusieurs reprises l'utilisation possible d'un « *numéro d'ordre* », déjà présent dans le précédent référentiel. Le ministère a précisé que l'utilisation d'un même numéro d'ordre dans différentes études était parfois nécessaire, notamment lorsque le projet nécessite d'effectuer plusieurs extractions pour mettre à jour les données.

Néanmoins, l'usage d'un tel numéro identifiant est à éviter afin de limiter le risque de réidentification entre différentes études où l'ordre serait similaire. Alerté sur ces risques, le ministère s'est engagé à prévoir également l'utilisation d'un identifiant aléatoire obtenu par un générateur de nombres pseudo-aléatoires cryptographiquement sûr.

En complément, la CNIL estime dans ce cas que le référentiel devrait préciser que :

– **l'usage d'un numéro d'ordre doit être limité aux cas où cela est strictement nécessaire et justifié ;**

– **si des tables de correspondance doivent être conservées, celles-ci devront faire l'objet de mesures techniques et organisationnelles renforcées.**

S'agissant du contrôle des systèmes du SNDS :

Concernant la périodicité des audits de cinq ans prévue par le projet de référentiel à la section 8.1, la CNIL prend acte de l'engagement du ministère de réduire ce délai à trois années.

Le ministère a également précisé qu'une procédure d'accréditation de prestataires, sous la responsabilité du comité d'audit, était envisagée pour la réalisation des audits externes. La CNIL prend acte de ce que le ministère s'est engagé à associer la CNIL à ses travaux sur la mise en œuvre d'une telle procédure.

Le précédent référentiel précisait en outre que les audits internes pouvaient être « *éventuellement délégués à des prestataires PASSI* » (prestataires d'audit de la sécurité des systèmes d'information). La CNIL recommande au ministère de réintégrer cette possibilité et d'imposer un recours systématique à de tels prestataires en cas de sous-traitance de ces audits.

Le projet de référentiel, en sa section 8.2, prévoit une revue des habilitations à la charge du seul responsable de traitement. La CNIL prend acte de l'engagement du ministère de compléter le projet de référentiel pour prévoir une revue des habilitations similaire par tout gestionnaire de système du SNDS, en particulier pour les administrateurs de ces systèmes.

Les autres dispositions du projet d'arrêté et du référentiel de sécurité annexé n'appellent pas d'observations en matière de protection des données.

La présidente,
M.-L. Denis