Projet de recommandation

Dossier patient informatisé (DPI)

Projet de recommandation soumis à consultation jusqu'au 16 mai 2025

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Fiche 1 : le contexte

1. La sensibilité des données traitées au sein des établissements de santé et leur volume requièrent la mise en place de mesures appropriées afin de protéger les données et respecter la vie privée des personnes.

2. Le déploiement accéléré et généralisé du numérique en santé ces dernières années a conduit à créer ou à étendre de nombreux systèmes d'information. Les récentes actualités de cybersécurité ont démontré l'intérêt que représentent ces données pour des tiers malveillants, ainsi que les faiblesses et limites des systèmes existants[1].

3. De plus, les violations de données touchant les établissements de santé peuvent avoir des conséquences significatives sur la vie privée des personnes concernées. En effet, l'indisponibilité des données peut conduire à un retard dans la prise en charge susceptible d'être qualifié de perte de chance pour le patient. Une atteinte à l'intégrité des données pourrait conduire à ce qu'une décision médicale inadaptée à la situation du patient, voire dangereuse, soit prise, par exemple si une allergie est mal renseignée dans le dossier patient. Enfin, une divulgation des données à des tiers non autorisés (par exemple la diffusion sur le web, accès par des tiers malveillants) constitue une atteinte au droit fondamental à la vie privée et une violation de l'obligation de secret professionnel à laquelle les établissements et les professionnels de santé sont tenus. Cette divulgation pourrait également conduire à la réutilisation de données personnelles en vue de personnaliser des messages d'hameçonnage, voire à des usurpations d'identité visant à obtenir d'autres informations médicales (par exemple, via une demande de droit d'accès).

4. Depuis plusieurs années la sécurité des données de santé est au cœur des travaux menés par la CNIL, que ce soit à travers sa politique de contrôles, les normes qu'elle adopte ou les différents avis et conseils rendus. Elle souhaite consolider dans un document unique les règles applicables aux dossiers patients informatisés.

5. Les exigences et bonnes pratiques décrites dans la présente recommandation reflètent les mesures de sécurité décrites dans le guide de la sécurité des données à caractère personnel (CNIL)[2] et dans le guide d'hygiène informatique (ANSSI)[3], dans leur dernière version publiée. La CNIL recommande la mise en place systématique des mesures décrites dans ces guides dès lors qu'elles sont applicables, indépendamment de l'analyse des risques.

6. La CNIL considère que les besoins de sécurité des DPI nécessitent en outre la mise en œuvre des mesures de sécurité spécifiques décrites dans la présente recommandation. Ces mesures peuvent par ailleurs être considérées comme des bonnes pratiques pour l'ensemble des traitements de données de santé à caractère personnel au sein de l'établissement.

7. Les établissements de santé devraient recourir à des logiciels DPI qui permettent de mettre en œuvre les mesures de sécurité décrites ci-après, ainsi que celles identifiées dans le cadre de leur analyse d'impact sur la protection des données (AIPD). Ces mesures devront être traduites en exigences à faire figurer dans les cahiers des charges pour les achats ou le développement de solutions logicielles. Une attention particulière devra enfin être portée au paramétrage des logiciels DPI afin que celui-ci corresponde aux besoins de sécurité et à la réalité des métiers.

8. Les droits des personnes concernées par un dossier patient informatisé sont partiellement abordés dans la présente recommandation. Ils feront l'objet de travaux approfondis ultérieurement afin de prendre en compte les évolutions introduites par le règlement relatif à l'espace européen des données de santé.

[1] Voir le rapport 2024 du CERT-FR sur le « Secteur de la santé - État de la menace informatique », ANSSI : https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-010/

[2] « Guide de la sécurité des données à caractère personnel », CNIL : https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

[3] Mesures de niveau « standard » du Guide d'hygiène informatique de l'Agence nationale de la sécurité des systèmes d'informations, Cyber.gouv.fr : https://cyber.gouv.fr/publications/guide-dhygiene-informatique

Fiche 2 : le périmètre de la recommandation

A. Quel est le traitement concerné par cette recommandation ?

10. Ce guide est dédié au traitement de données à caractère personnel mis en œuvre :
    - par un **établissement de santé, public ou privé,** tel que défini à l'article L. 6111-1 du code de la santé publique (CSP), ci-après le responsable de traitement ;
    - à des fins d'enregistrement et de conservation des données à caractère personnel collectées à l'occasion d'une prise en charge sanitaire, médico-sociale ou des activités nécessaires à la coordination de ces prises en charge.

    Ce traitement est dénommé ci-après « dossier patient informatisé ».

11. Le présent guide ne vise pas :
    - les traitements mis en œuvre par des professionnels de santé exerçant à titre libéral, quel que soit leur lieu d'exercice, à des fins de gestion du dossier patient et de gestion administrative de leur patientèle (par exemple exercice libéral en établissement de santé, exercice libéral en ville). Ces professionnels pourront se référer au référentiel « cabinet médical et paramédical » adopté par la CNIL ;
    - les traitements mis en œuvre par un établissement de santé aux fins de facturation et de remboursement par les organismes d'assurance maladie obligatoire ou complémentaire ;
    - les traitements mis en œuvre par un établissement de santé à des fins de production et d'analyse d'imageries médicales ;
    - les traitements mis en œuvre par un établissement de santé pour l'analyse d'échantillons biologiques dans un service d'anatomopathologie ;
    - les traitement mis en œuvre par un établissement de santé à des fins de gestion de l'activité d'une pharmacie à usage intérieur (PUI) ;
    - les traitements mis en œuvre par un établissement de santé à des fins d'analyse d'échantillons biologiques dans un service de biologie médicale ;
    - les traitements mis en œuvre par un établissement de santé à des fins de télésanté au sens des articles L. 6316-1 et L. 6316-2 du CSP ;
    - les traitements mis en œuvre par un établissement de santé lors de l'utilisation d'un dispositif médical, lorsque les données sont collectées au sein du logiciel associé au dispositif médical et en amont de leur enregistrement dans le DPI ;
    - les traitements mis en œuvre par un établissement de santé à des fins de création d'un entrepôt de données dans le domaine de la santé ;
    - les traitements mis en œuvre à des fins d'analyse de l'activité médicale des établissements de santé prévu à l'article L. 61113-7 du CSP ;
    - les traitements mis en œuvre à des fins de recherche, étude ou évaluation dans le domaine de la santé ;
    - le dossier médical partagé (DMP)[4].

B. À qui s'adresse la recommandation ?

12. Il s'adresse en premier lieu au **responsable de traitement et leurs représentants légaux qui sont tenus de garantir la conformité du DPI** vis-à-vis de la règlementation et de l'état de l'art en matière de sécurité informatique**.**

13. Plus précisément, il est **destiné à l'usage des délégués à la protection des données** (DPO), des conseils en matière de protection des données personnelles, du médecin responsable de l'information médicale et **des responsables de systèmes d'information** (DSI, RSSI) du responsable de traitement.

14. **Au regard des rôles essentiels joués par les sous-traitants et les éditeurs de services numériques** (logiciel, système d'information, *etc.*) dans la conformité et la sécurité du DPI**, ces acteurs sont invités à prendre connaissance de ce guide.** Les recommandations formulées leur permettront, chacun à leur niveau, de garantir et/ou fournir les moyens nécessaires permettant de démontrer que leurs produits et/ou leurs services sont sûrs et conformes à la règlementation applicable.

[4] « Santé et prévention : Le dossier médical partagé (DMP) », Ameli : https://www.ameli.fr/medecin/sante-prevention/dmp-et-mon-espace-sante/dossier-medical-partage/dmp-en-pratique

Fiche 3 : la responsabilité de traitement

15. **Le responsable de traitement du DPI est l'établissement de santé au sein duquel la personne a été prise en charge**.

16. Dans l'hypothèse d'une responsabilité conjointe de traitement entre plusieurs établissements de santé (notamment dans le cadre de groupement hospitalier de territoire), ceux-ci doivent définir leurs obligations respectives dans le cadre d'une convention conforme à l'article 26 du RGPD. Cet accord devra tenir compte de la règlementation nationale applicable et notamment celle relative au secret professionnel.

17. Aussi, cette responsabilité conjointe de traitement ne devrait pas permettre l'accès par le personnel d'un établissement aux données à caractère personnel des patients pris en charge dans un autre établissement, sauf si ce personnel peut être qualifié de membre de l'équipe de soins au sens de l'article L. 1110-12 du CSP.

Fiche 4 : la base légale

18. Les établissements de santé sont tenus de mettre en œuvre et de conserver les données à caractère personnel des patients qu'ils prennent en charge (articles R. 1112-2 et R. 1112-7 du CSP). Ces traitements sont donc nécessaires au **respect d'une obligation légale à laquelle le responsable de traitement est soumis** (article 6.1.c) du RGPD).

19. Dans ce cadre, le traitement de données sensibles, dont des données concernant la santé, est **nécessaire aux fins de la médecine préventive, de diagnostics médicaux, de la prise en charge sanitaire** ou sociale, ou de la gestion des systèmes et des services de soins (article 9.2.h) du RGPD).

20. Au regard de la base légale du traitement de données, la personne ne dispose pas du droit :

    - de s'opposer au traitement de ses données ;
    - de demander leur effacement ;
    - à la portabilité de leurs données.

    Les personnes devront être informés de ces limitations à leurs droits.

21. Le responsable de traitement doit veiller à assurer la confidentialité des données du DPI notamment en rendant possible la restriction des accès à l'identité réelle du patient (par exemple, pour protéger la vie privée d'une personnalité publique, d'un patient dont des proches exercent dans l'établissement ; voir la Fiche 13 – Partie B).

Fiche 5 : la gouvernance, l'analyse d'impact et l'homologation

22. La réglementation applicable à tous les traitements de données à caractère personnel impose aux responsables de traitement de mettre en œuvre des mesures afin de garantir la sécurité (confidentialité, intégrité, disponibilité) des données à caractère personnel traitées et la résilience des systèmes informatiques. En effet, l'indisponibilité des données peut conduire à un retard dans la prise en charge, susceptible d'être qualifié de perte de chance pour le patient. Une atteinte à l'intégrité des données pourrait conduire à ce qu'une décision médicale inadaptée à la situation du patient, voire dangereuse, soit prise. Enfin, une divulgation des données à des tiers non autorisés (par exemple la diffusion sur le web, accès par des tiers malveillants) constitue une atteinte au droit fondamental à la vie privée et une violation de l'obligation de secret professionnel auquel les établissements et les professionnels de santé sont tenus. Cette divulgation pourrait également conduire à la réutilisation de données personnelles en vue de personnaliser des messages d'hameçonnage, voire à des usurpations d'identité visant à obtenir d'autres informations médicales (par exemple, via une demande de droit d'accès).

23. Plus précisément, les traitements de données à caractère personnel doivent s'appuyer sur des mesures permettant d'assurer un niveau de sécurité satisfaisant au regard de l'obligation prévue par les articles 5.1.f et 32 du RGPD. Celle-ci, qui prend la forme d'une obligation de moyens renforcée, impose d'adopter une approche par les risques pour adapter les mesures de sécurité en fonction des risques pour les personnes concernées.

24. Le RGPD prévoit que le responsable de traitement doit être en mesure de démontrer, à toute étape du cycle de vie d'un traitement, sa conformité à la règlementation applicable et notamment que les mesures de sécurité mises en œuvre sont appropriées aux risques (article 5.2 et 24 du RGPD).

25. À cet égard, le **DPI doit faire l'objet d'une analyse d'impact relative à la protection des données** (AIPD)[5]. L'AIPD constitue un élément essentiel pour répondre aux exigences du RGPD concernant notamment la mise en œuvre de mesures de sécurité proportionnées aux risques (articles 5.1.f) et 32).

26. Cette AIPD doit être **mise à jour régulièrement** afin de prendre en compte l'évolution des risques pesant sur le DPI et le cadre juridique applicable. En particulier, une mise à jour devra intervenir à chaque changement majeur du DPI, de son contexte ou de la menace, susceptible d'avoir une incidence sur les risques. **La CNIL recommande que l'AIPD soit revue annuellement**.

27. Le responsable de traitement est tenu d'inscrire le traitement de données à caractère personnel lié au DPI sur son **registre d'activité de traitement**. Un modèle de registre simplifié est disponible sur le site web de la CNIL[6].

28. Pour les systèmes d'information de l'Etat et de ses établissements publics, dont les établissements publics de santé, une **homologation de sécurité doit être réalisée**[7]. Pour les établissements privés de santé, la CNIL recommande de mettre en œuvre une procédure d'homologation.

[5] *Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise* (PDF, 228 ko), CNIL : https://www.cnil.fr/sites/cnil/files/atoms/files/liste-traitements-aipd-requise.pdf

[6] « Le registre des activités de traitement », CNIL : https://www.cnil.fr/fr/RGPD-le-registre-des-activites-de-traitement

[7] Article 4-3 du décret n°2019-1088 du 25 octobre 2019 modifié, Légifrance : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039281619

29. La méthode décrite ci-après permet de guider la réalisation de l'homologation :

- se conformer à la **méthode recommandée par l'Agence nationale de la sécurité des systèmes d'information** (ANSSI)[8]. Celle-ci implique de faire valider par une personne habilitée à engager l'établissement, généralement le directeur général, le niveau de sécurité du système, les risques résiduels identifiés et l'éventuel plan d'action complémentaire permettant d'améliorer la couverture des risques ;
- mettre en place une **gouvernance dédiée et durable à l'échelle de l'établissement**, avec le soutien de la direction de l'établissement ;
- mettre en place une démarche de gestion des risques méticuleuse et suivie par la direction lors de points réguliers, *a minima* annuels. **Les risques pesant sur le DPI doivent être précisément identifiés** ;
- traiter les risques identifiés **à l'aide de mesures adéquates, précises et suivies dans le temps**. La CNIL recommande en outre qu'un **plan d'action soit formalisé et soumis pour approbation à la direction de l'établissement**, qui engage les moyens nécessaires (humains, techniques, financiers). Une bonne pratique consiste à assurer le suivi du plan d'action et à le mettre à jour mensuellement.

30. En particulier, il convient de prendre en compte les scénarios de risques suivants :

- compromission de personnes habilitées à accéder au traitement, notamment ceux disposant de privilèges élevés ;
- compromission de prestataires chargés du développement informatique, de sa mise en œuvre, de l'hébergement ou bien des opérations de maintenance ou de support ;
- compromission de composants techniques pouvant prendre le contrôle du DPI, tels que les annuaires d'entreprise[9] ;
- compromission du socle technique dont dépend le DPI (serveurs, actifs réseaux, mécanisme de réplication de données, robot de sauvegarde, etc.).

Cette analyse peut s'appuyer sur la méthode « EBIOS Risk Manager » de l'ANSSI qui aide à identifier et prioriser les principaux chemins d'attaque sur le système considéré, et à déterminer les mesures adéquates pour s'en protéger[10].

31. Ces recommandations, ainsi que celles contenues dans l'ensemble du présent guide, sont sans préjudice des exigences spécifiques fixées par la loi ou la règlementation lorsque le DPI est mis en œuvre par un établissement ayant un statut d'opérateur d'importance vitale (OIV) au sens de la loi de programmation militaire de 2013 ou d'entité essentielle au sens de la directive NIS 2[11]. Elles peuvent toutefois les compléter au regard des enjeux particuliers des données à caractère personnel du DPI, qui ne sont pas l'objet des textes précités.

[8] « Homologation de sécurité », ANSSI : https://cyber.gouv.fr/lhomologation-de-securite

[9] Par exemple, un composant « Active Directory »

[10] « Méthode EBIOS Risk Manager », ANSSI : https://cyber.gouv.fr/la-methode-ebios-risk-manager

[11] « Directive NIS 2 », EUR-Lex : https://eur-lex.europa.eu/eli/dir/2022/2555

Fiche 6 : les données composant le dossier patient informatisé

32. L'**ensemble des données à caractère personnel collectées à l'occasion d'une prise en charge sanitaire**, médico-sociale ou des activités nécessaires à la coordination de ces prises en charge **sont des données couvertes par le secret professionnel** mentionné à l'article L. 1110- 4 du CSP.

33. **Toutes les données administratives et les données sensibles, dont les données concernant la santé, d'une personne**, bénéficiant ou appelée à bénéficier d'un acte diagnostique, thérapeutique, de prévention, de soulagement de la douleur, de compensation du handicap ou de prévention de la perte d'autonomie, ou d'interventions nécessaires à la coordination de plusieurs de ces actes **doivent être référencées avec l'identifiant national de santé** (INS). Aucun autre identifiant ne peut être utilisé pour le référencement sauf en cas d'impossibilité d'accéder à l'INS et afin de ne pas empêcher la prise en charge sanitaire et médico-sociale de la personne. L'identification des personnes prises en charge doit être réalisée conformément au référentiel « Identifiant national de santé » ainsi que le référentiel national d'identitovigilance[12].

34. Toutes les données collectées ou produites à l'occasion d'une activité de télésanté ou lors de l'utilisation d'un dispositif médical constituent par nature des données du DPI, sous réserve qu'elles soient nécessaires à la prise en charge de la personne.

35. La présente fiche est divisée en plusieurs parties qui correspondent à l'infrastructure technique recommandée par la CNIL. Cette division ne correspond pas à l'interface logicielle visible par un utilisateur.

36. Chaque partie détaille les données concernées ainsi que les mesures de sécurité requises ou recommandées s'agissant des données administratives du patient et ses proches (A), des données administratives des professionnels (B), les données structurées liées à la prise en charge (C) et les documents du DPI qui contiennent des données administratives et des données sensibles(D). Les mesures décrites dans la présente fiche sont axées sur le stockage des informations ; elles s'articulent avec celles de la Fiche 13 concernant les habilitations d'accès.

C. Les données administratives relatives au patient et à ses proches

1. Quelles sont les données concernées ?

a. Les données relatives au patient

37. L'INS de chaque personne prise en charge ou appelée à être prise en charge doit être traité. Cet identifiant correspond au numéro d'inscription au répertoire national d'identification des personnes physique (NIR) ou, pour les personnes en instance d'attribution d'un NIR, au numéro d'identification d'attente (NIA). Le référentiel « identifiant national de santé »[13] précise les cas résiduels dans lesquels un autre identifiant peut être utilisé.

38. Un numéro d'identifiant permanent du patient (IPP) ou un numéro d'identifiant de l'épisode de soin (IEP) peuvent être utilisés localement sous réserve que les données concernant la santé soient référencées par l'INS.

[12] « Référentiel Identifiant National de Santé », Agence du numérique en santé (ANS) : https://esante.gouv.fr/referentiel/identite-nationale-de-sante

[13] « Référentiel INS », ANS : https://esante.gouv.fr/produits-services/referentiel-ins

39. Les données administratives relatives aux patients pouvant être traitées incluent en particulier :

- nom, prénoms ;
- genre, civilité ;
- date et lieu de naissance ;
- date et lieu de décès ;
- coordonnées téléphoniques, électroniques et adresse de résidence ;
- photographie, sous réserve du respect du droit à l'image ;
- régime d'affiliation à l'assurance maladie obligatoire et à l'assurance complémentaire (mutuelle, assurance privée).

b. Les données relatives aux proches du patient

40. Si le patient a désigné une personne de confiance définie à l'article L. 1111-6 du CSP ou a désigné une personne à prévenir, les données suivantes peuvent être traitées :

- nom, prénoms ;
- civilité ;
- coordonnées téléphoniques et électroniques.

41. Si le patient est une personne mineure ou personne majeure faisant l'objet d'une mesure de protection, les données suivantes peuvent être traitées :

- nom, prénoms ;
- civilité ;
- lien de rattachement (titulaire de l'autorité parentale, tuteur, curateur, mandataire) ;
- coordonnées téléphoniques et électroniques.

2. Les mesures de sécurité associées

42. **Les données administratives des patients et de leurs proches doivent être stockées de manière cloisonnée** par rapport aux données de santé liées à la prise en charge des patients.

43. Ce cloisonnement permet d'utiliser les données administratives pour d'autres finalités que la prise en charge sanitaire, notamment la facturation des prestations, sans divulguer l'ensemble des données de santé (seule la codification des actes et médicaments est transmise). Il permet également de limiter les impacts en cas d'accès illégitime aux données de santé, qui ne contiendront pas de données directement identifiantes ou de coordonnées.

44. **La CNIL recommande que la base administrative repose sur des systèmes et bases de données distincts des données de santé**, par exemple dans un système dédié de gestion administrative du malade (GAM), et que ses données soient chiffrées à l'aide de clés spécifiques, gérées de manière distincte. Les algorithmes utilisés et les modalités de gestion des clés associées doivent être conformes au référentiel général de sécurité (annexes B1 et B2)[14] et aux recommandations de l'ANSSI[15] afin d'assurer un cloisonnement effectif et robuste.

c. Cas particulier du NIR/INS

45. Le NIR est stocké dans la base administrative aux fins de facturation, de même que l'INS pour assurer l'identification exacte du patient et de ses données dans le cadre du référentiel identifiant national de santé et du référentiel national d'identitovigilance[16].

[14] « Référentiel général de sécurité (RGS) », ANSSI : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents

[15] « Mécanismes cryptographiques », ANSSI : https://cyber.gouv.fr/publications/mecanismes-cryptographiques

[16] « Référentiel national d'identitovigilance », ANS : https://esante.gouv.fr/produits-services/referentiel-ins

46. **Le NIR et l'INS constituent, par leur nature et leur usage, des identifiants qui doivent faire l'objet d'une protection renforcée**, en particulier des habilitations d'accès spécifiques et une traçabilité renforcée. Ils pourraient faire l'objet d'un chiffrement spécifique au sein de la base administrative, avec une clé dédiée différente de celle de la base administrative.

47. Dans le cadre de l'identitovigilance, les échanges de données contenant l'INS et les traits d'identité doivent être réalisés sur des canaux de communication sécurisés afin d'en garantir la confidentialité et l'intégrité. La CNIL recommande que ces canaux soient protégés par des mesures de chiffrement et d'authentification de l'émetteur et du destinataire, qui soient adaptées aux risques et conformes au référentiel général de sécurité[17] et aux recommandations de l'ANSSI[18].

D. Les données administratives relatives aux professionnels de santé

1. Quelles sont les données concernées ?

48. Les professionnels concernés sont les suivants :

- les professionnels exerçant dans l'établissement de santé au sein duquel la personne a été prise en charge sous réserve qu'ils aient participé à la prise en charge de la personne ;
- le médecin traitant du patient ;
- les professionnels de santé hors établissement de santé, qui ont pris en charge la personne dans le cadre de l'épisode de soin.

49. Les données à caractère personnel pouvant être traitées sont notamment les suivantes :

- données d'identification : nom, prénom, titre ;
- fonction, service et unité d'exercice ;
- coordonnées professionnelles (adresse électronique et numéro de téléphone professionnels) ;
- numéro ADELI ou numéro RPPS.

2. Les mesures de sécurité associées

50. **La CNIL recommande que les données administratives des professionnels de santé soient stockées de manière cloisonnée** par rapport aux données de santé liées à la prise en charge des patients.

51. Ceci permet de limiter les impacts en cas d'accès illégitime aux données de santé, car l'indication des noms des professionnels assurant la prise en charge d'un patient est susceptible de faciliter ou de confirmer sa réidentification par une personne malveillante.

E. Les données structurées liées à la prise en charge

1. Quelles sont les données concernées ?

52. Des données à caractère personnel comprenant des données concernant la santé et d'autres données sensibles, selon les contextes peuvent être traitées **sous réserve qu'elles soient strictement nécessaires à la prise en charge sanitaire, au suivi des personnes ou à des activités nécessaires à la coordination de cette prise en charge**. Toutes les informations révélées par le patient lors de sa prise en charge ne doivent pas nécessairement intégrer son dossier : **il convient de traiter uniquement les données utiles pour son suivi. En tout état de cause, il appartient au professionnel de santé prenant en charge la personne d'apprécier les données nécessaires pour l'exercice de ses missions.**

53. Les données liées à la prise en charge peuvent provenir :

- de la personne elle-même ;
- d'un professionnel de santé ayant participé à la prise en charge de la personne ;

[17] « RGS », ANSSI : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents
[18] « Mécanismes cryptographiques », ANSSI : https://cyber.gouv.fr/publications/mecanismes-cryptographiques

- d'un tiers (par exemple un proche du patient).

54. S'agissant de tout patient pris en charge par un établissement de santé, les données à caractère personnel suivantes peuvent être traitées, sous réserve qu'elles soient strictement nécessaires à la prise en charge sanitaire de la personne (liste non-exhaustive) :

    - poids, taille ;
    - sexe ;
    - caractéristiques des rendez-vous médicaux (date, service, professionnel de santé) ;
    - données relatives à un acte médical, paramédical, de biologie médicale, etc. ;
    - données relatives aux effets et événements indésirables ;
    - données relatives aux produits de santé utilisés dans la prise en charge de la personne ou prescrits (notamment date d'administration ou d'utilisation, dénomination du produit, posologie, *etc.*) ;
    - observations médicales et paramédicales ;
    - données issues de dispositifs médicaux ou d'appareils de mesure ;
    - données relatives aux transfusions sanguines ;
    - antécédents personnels et/ou familiaux, maladies ou événements associés (dont les données liées aux vaccinations antérieures) ;
    - allergies connues ;
    - photographie et/ou vidéo et/ou enregistrement vocal recueillis dans des conditions conformes aux dispositions applicables en matière de droit à l'image et de droit à la voix. Il conviendra de déterminer si l'identification de la personne est nécessaire à la prise en charge ;
    - consommation de tabac, alcool, drogues ;
    - statut vital et cause du décès ;
    - selon le contexte :
        - données génétiques ;
        - orientation et vie sexuelle ;
        - données révélant l'origine ethnique ;
        - données relatives à la situation familiale (situation matrimoniale, nombre d'enfants) ;
        - données relatives à la vie professionnelle (profession, conditions de travail) ;
        - déplacements (p. ex. : vers le lieu de soin : mode, durée) ;
        - habitudes de vie et comportements, par exemple : dépendance (seul, en institution, autonome, grabataire), assistance (aide-ménagère, familiale), exercice physique (intensité, fréquence, durée), régime et comportement alimentaire, loisirs ; mode de vie (p.ex. : urbain, semi-urbain, nomade, sédentaire), habitat (maison particulière, immeuble, étage, ascenseur, etc.) ;
        - échelle de qualité de vie ou autres informations sur la qualité de vie de la personne ;
        - exposition à des risques sanitaires connus (physiques, chimiques, biologiques et environnementaux, etc.) ;
        - participation à une recherche impliquant la personne humaine, dès lors que celle-ci est susceptible d'avoir un impact sur la prise en charge.

55. Il est précisé que, pour les patients hospitalisés dans un établissement de santé, le DPI doit *a minima* contenir les informations mentionnées à l'article R. 1112-2 du CSP.

56. Les données génétiques mentionnées ici visent celles strictement nécessaires à la prise en charge du patient, comme composante de son parcours de soin. Par exemple, l'indication d'une mutation caractéristique d'une maladie dont souffre le patient pourra figurer directement dans les données structurées, tandis que le résultat d'un séquençage génétique complet sera versé dans les documents du DPI (voir la partie D).

2. Les mesures de sécurité associées

57. **Les données structurées du DPI liées à la prise en charge doivent être cloisonnées par rapport aux données administratives et stockées sous forme pseudonymisée**. Elles ne comportent pas de données directement identifiantes mais sont référencées par l'identifiant permanent du patient (IPP), qui fait le lien avec ses données administratives, et par l'identifiant des professionnels de santé ayant participé à la prise en charge. La CNIL recommande que l'IPP soit généré via une méthode[19] qui ne permette pas à un tiers de le déduire à partir de traits d'identité du patient ni à partir de son historique médical dans l'établissement.

F. Les documents du DPI

1. Qu'est-ce qu'un document du DPI ?

58. Les données à caractère personnel mentionnées *Supra* (A, B et C) peuvent figurer sur des documents dans un format informatique non structuré au sein de documents dans un format informatique non structuré qui ont vocation à être remis au patient ou à un professionnel participant à la prise en charge. Il s'agit par exemple des documents produits à l'occasion d'une prise en charge tels que des comptes-rendus, des résultats d'examens, des fiches de liaison, des ordonnances, etc.

59. En application de l'article R. 1112-3 du CSP, chaque document du DPI doit :

- être daté ;
- comporter l'identité du patient (nom, prénom et date de naissance) et son numéro d'identification (INS ainsi qu'un éventuel identifiant local – IPP ou IEP) ;
- comporter l'identité du professionnel de santé (nom, prénom et numéro RPPS[20]) ayant collecté les données à caractère personnel et/ou produit le document.

2. Les mesures de sécurité associées

60. Les documents du DPI comportent à la fois des données directement identifiantes du patient et de tiers et des professionnels de santé, et des données de santé du patient. Il s'agit par exemple des documents produits à l'occasion d'une prise en charge tels que des comptes-rendus, des résultats d'examens, des fiches de liaison, des ordonnances, etc.

61. La CNIL recommande que ces documents **soient stockés de manière cloisonnée autant vis-à-vis des données de santé structurées que des données administratives**. Ceci est facilité par le fait qu'ils sont généralement stockés dans des systèmes ou sous-systèmes dédiés (GED[21] pour les documents textuels et PACS[22] pour l'imagerie), dont il faut néanmoins assurer la sécurité au même niveau que le reste du DPI, dont ils font partie du périmètre, ainsi qu'un cloisonnement effectif et robuste.

[19] Fonction de hachage cryptographique résistante aux attaques par force brute, ou générateur de nombres pseudo-aléatoires cryptographiquement sûr.
[20] Ou, dans l'attente du déploiement complet du RPPS+, tout autre identifiant sectoriel applicable (par exemple le numéro ADELI)
[21] GED : Gestion électronique de documents
[22] PACS : *Picture Archiving and Communication System*

a. Cas particulier des données génétiques

62. Les données génétiques qui ne sont pas directement déductibles du diagnostic d'une pathologie du patient doivent faire l'objet d'une protection renforcée car leur accès par une personne malveillante présente des risques majeurs pour la vie privée du patient et de ses proches, bien au-delà du périmètre de soin pour lequel elles ont été recueillies. C'est notamment le cas pour les données résultant du séquençage complet du génome du patient ou d'une tumeur, ou résultant d'un criblage large de marqueurs génétiques. **La CNIL recommande que les fichiers de données génétiques soient protégés par un chiffrement spécifique**.

b. Cas particulier des documents issus du DMP et d'autres systèmes d'information/traitements

Problème constaté :

DPI récupérant systématiquement l'historique des remboursements des patients auprès des téléservices de l'Assurance Maladie, en les conservant sur les douze derniers mois.

63. Conformément au référentiel DMP, les documents issus du DMP et stockés dans le DPI doivent faire l'objet d'une protection renforcée, équivalente à celle qu'ils avaient au sein du DMP[23]. Pour atteindre ce niveau de sécurité, la CNIL recommande de mettre en œuvre l'ensemble de la présente recommandation, en particulier les mesures incontournables que constituent l'authentification multifacteur, la gestion des habilitations et la traçabilité des accès au DPI telles que décrites dans la Fiche 13.

64. De manière générale, seuls les documents pertinents pour la prise en charge d'un patient doivent être copiés dans le DPI depuis le DMP. Ils **doivent faire l'objet d'un marquage spécifique**, de préférence inséré de manière visible dans le document lui-même sans perturber son contenu médical. Ce marquage devrait :

- indiquer la provenance et la date du document ;
- alerter les utilisateurs sur la nécessité de s'assurer qu'il est à jour ;
- alerter les utilisateurs sur la nécessité de le manipuler en respectant des mesures de sécurité adéquates.

65. Dans certains cas, le professionnel responsable de la prise en charge peut être amené, en vue de préparer un épisode de soins, à précharger temporairement à partir du DMP les informations qui lui paraissent pertinentes et nécessaires pour la prise en charge, avec un filtrage sur des critères pré-paramétrés (patient, type, date, auteur, *etc.*). **L'accès au DMP via le DPI** (mode intégré ou mode contextuel) **doit être réalisé après une authentification multifacteur du professionnel demandeur. Le DPI doit alors permettre d'assurer que seul le professionnel demandeur a accès aux informations du DMP** qu'il a intégrées temporairement dans le DPI. Celles-ci seront préchargées au plus tôt trois jours avant la prise en charge et, sans action manuelle du professionnel pour les enregistrer durablement dans le DPI, seront supprimées automatiquement après l'épisode de soins ou au plus tard trois jours après leur préchargement.

66. Plutôt que les documents eux-mêmes, **la CNIL recommande que le DPI permette d'importer uniquement une liste temporaire de leurs caractéristiques principales** (typologie métier, date, source, auteur, version) et propose ensuite leur visualisation à la demande, de manière ergonomique sans quitter l'interface utilisateur du DPI (par exemple, en utilisant des API[24] sécurisées).

67. De manière générale, **la CNIL recommande d'appliquer à tous les documents provenant de sources externes au DPI les mesures prescrites pour ceux provenant du DMP**, en particulier la limitation aux seuls documents pertinents et le marquage de leur provenance.

[23] « Référentiel de sécurité et d'interopérabilité relatif à l'accès des professionnels au dossier médical partagé (DMP) », Légifrance : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048368244

[24] Interfaces de programmation d'application, qui font l'objet d'une recommandation de la CNIL. « La CNIL publie une recommandation relative au partage de données par API », CNIL : https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-technique-relative-au-partage-de-donnees-par-api

Fiche 7 : les mesures de sécurité générales liées à la conservation des données

A. Chiffrement des données

68. Le chiffrement des données joue un rôle important dans la protection des données personnelles et la sécurité d'un système d'information. Lorsque l'algorithme de chiffrement et la gestion des clés cryptographiques associées sont à l'état de l'art, le chiffrement permet de garantir la confidentialité des données conservées et d'assurer leur défense en profondeur dans le cas d'une attaque sur le système d'information ou sur le matériel qui le supporte. Sa mise en œuvre peut être facilitée par les logiciels et matériels récents qui incluent nativement des fonctionnalités de chiffrement (par exemple, les serveurs et baies de disques durs, les systèmes de gestion de bases de données, etc.).

69. Par conséquent, **les données du DPI devraient être chiffrées au repos** avec des algorithmes, tailles et modalités de gestion de clé conformes au référentiel général de sécurité (annexes B1 et B2)[25] et aux recommandations de l'ANSSI[26]. Une procédure opérationnelle de gestion des clés devrait alors être formalisée, assurant notamment la protection des secrets, le maintien de leur disponibilité en cas d'incident touchant le système d'information (par exemple, via une sauvegarde distincte), ainsi que leur renouvellement en cas de compromission.

B. Sauvegardes régulières, protégées et testées

Problèmes constatés :

- Sauvegardes rendues inaccessibles par un rançongiciel, qui a pu les atteindre et les chiffrer car elles étaient connectées et « en ligne ».
- Contrat d'hébergement HDS n'intégrant pas de sauvegarde, sans que l'établissement en soit conscient.
- Dégâts importants sur un site d'hébergement, ayant rendu inaccessibles les sauvegardes stockées dans un bâtiment voisin.

70. Les données du DPI doivent faire l'objet d'un **plan assurant une sauvegarde régulière des données**, permettant leur restauration et la reprise d'activité en cas d'incident. Le plan doit prendre en compte :

- la perte de données maximale admissible, liée à l'écart entre l'heure de la dernière sauvegarde et le moment de l'incident ;
- la durée maximale d'interruption admissible, liée au temps de restauration des données et de remise en fonctionnement du système.

Si ces valeurs, définies avec les métiers, sont inférieures à la journée, la CNIL recommande de considérer des solutions de réplication en plus de la sauvegarde classique. Cette dernière demeure cependant nécessaire car la réplication de données, constamment connectée par nature, est vulnérable à des attaques en intégrité et en disponibilité (rançongiciels, par exemple).

71. Pour rétablir dans leur exactitude les données des patients suite à un incident sur le DPI ayant provoqué la perte des enregistrements les plus récents, il est nécessaire de mettre en place une procédure permettant :

- d'identifier les dossiers patients incomplets et de les marquer comme tels ;
- d'organiser et d'effectuer la ressaisie des données manquantes ou obsolètes.

[25] « RGS », ANSSI : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents

[26] « Mécanismes cryptographiques », ANSSI : https://cyber.gouv.fr/publications/mecanismes-cryptographiques

La CNIL recommande de procéder avec l'aide des professionnels de santé et des personnes concernées (par exemple dans le cadre de documents échangés avec le patient), dès que possible après la résolution de l'incident, et sinon à l'occasion des prochains actes et interactions avec les patients sur ces dossiers.

72. Afin de protéger les données sauvegardées, notamment contre des attaques de rançongiciels, la CNIL encourage à appliquer les recommandations de l'ANSSI concernant la sauvegarde des systèmes d'information[27]. En particulier, les sauvegardes devraient disposer d'une zone réseau isolée de la zone de production et faire l'objet d'habilitations et de droits d'accès spécifiques, restreints à un nombre limité de personnes (administrateurs des systèmes d'information, par exemple). Elles doivent de plus être stockées à distance du centre d'hébergement principal et être protégées physiquement et logiquement contre le vol, la perte, les accès illégitimes et toute altération malveillante ou accidentelle. Des tests de restauration effectués régulièrement, *a minima* chaque trimestre, sont fortement recommandés.

73. En outre, **la CNIL recommande que les sauvegardes soient chiffrées** conformément au référentiel général de sécurité (annexes B1 et B2) [28] et aux recommandations de l'ANSSI[29]. Une gestion spécifique devrait être prévue pour protéger l'accès aux clés et conserver celles-ci afin qu'elles soient toujours disponibles au moment d'une restauration (par exemple, avec des habilitations spécifiques et un système de stockage dédié).

[27] « Sauvegarde des systèmes d'information », ANSSI : https://cyber.gouv.fr/publications/fondamentaux-sauvegarde-systemes-dinformation
[28] « RGS », ANSSI : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents
[29] « Mécanismes cryptographiques », ANSSI : https://cyber.gouv.fr/publications/mecanismes-cryptographiques

Fiche 8 : les durées de conservation

Problèmes constatés :

- Des données à caractère personnel sont conservées sans limite de durée.
- Des dates de purges sont prévues uniquement après la première consultation d'un enregistrement (pas de purge si jamais consulté).
- Une purge manuelle est prévue mais n'est pas effectuée régulièrement, faute de temps de la part des utilisateurs ou des administrateurs.

1. Quels sont les principes ?

75. En application de l'article R. 1112-7 du CSP, les données du DPI doivent être conservées en base active pendant une durée maximale de[30] :

    - **20 ans à compter du dernier passage dans l'établissement (hospitalisation ou consultation)**. Lorsque la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date ;
    - **10 ans à compter du décès de la personne**, si celui-ci est intervenu moins de 10 ans après son dernier passage dans l'établissement.

76. Il convient également de prendre en compte les **règles spécifiques** susceptibles de s'appliquer à chaque dossier. En effet, la nature de la prise en charge peut nécessiter la conservation des données pour des durées plus longues, comme c'est le cas par exemple pour le dossier transfusionnel[31] ou encore en matière d'assistance médicale à la procréation[32].

77. Il appartient à chaque responsable de traitement d'évaluer, notamment pour les cas particuliers (décès du patient, déménagement, prise en charge en maternité, etc.), **l'opportunité d'archiver les données en base intermédiaire**. Il est recommandé de formaliser une procédure à cet égard. En tout état de cause, la durée de conservation en base intermédiaire ne pourra pas dépasser les durées prévues par le CSP rappelées *Supra*.

78. **A l'issue de ces délais,** la décision de destruction du dossier médical est prise par le directeur de l'établissement après avis du médecin responsable de l'information médicale (médecin DIM).

79. Des règles particulières de conservation des archives publiques prévues par le code du patrimoine peuvent trouver à s'appliquer concernant les données des DPI. Les responsables de traitement sont invités à s'assurer qu'ils ne relèvent pas du champ d'application de cette règlementation.

80. Le DPI comprend également des **traces fonctionnelles et techniques** dont les modalités et durées de conservations sont abordées dans la Fiche 13 – Partie C.

2. Les mesures de sécurité associées

81. **Des procédures automatiques ou manuelles doivent permettre d'assurer l'archivage intermédiaire des données du DPI, complétées de procédures manuelles pour leur purge à la fin de leur durée de conservation**, en tenant compte de la règlementation applicable.

82. La CNIL recommande que le logiciel DPI et son système de base de données permettent de définir une périodicité de déclenchement automatique et des critères techniques d'archivage intermédiaire, basés sur la typologie des données et sur des dates, qui peuvent être fonctionnelles (par exemple, une date de soins) ou techniques (par exemple, un horodatage automatique des modifications de données) afin de respecter les durées de conservation définies en base active.

[30] Pour plus d'informations : « Référentiel de la CNIL sur les durées de conservation des traitements dans le domaine de la santé (hors recherches) », CNIL : https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_-_traitements_dans_le_domaine_de_la_sante_hors_recherches.pdf

[31] INSTRUCTION N° DGS/PP4/DGOS/PF2/2021/230 du 16 novembre 2021 relative à la réalisation de l'acte transfusionnel.

[32] Voir point I-4.3 de l'arrêté du 5 octobre 2023 modifiant l'arrêté du 11 avril 2008 relatif aux règles de bonnes pratiques cliniques et biologiques d'assistance médicale à la procréation et abrogeant l'arrêté du 30 juin 2017 modifiant l'arrêté du 11 avril 2008.

83. L'intégration des fonctionnalités d'archivage et de purge dès la phase de conception d'une version majeure du logiciel DPI favorise significativement leur faisabilité technique lors de la phase de développement. S'il n'est pas possible de supprimer certains enregistrements, par exemple en raison de contraintes d'intégrité des données sur un système déjà existant, leur contenu peut être remplacé par des valeurs vides ou non signifiantes.

Fiche 9 : la sécurisation des échanges de données

84. Les échanges de données, plus ou moins automatisés, entre le DPI, les systèmes de gestion des laboratoires de biologie médicale, internes et externes, les systèmes d'imagerie médicale, les dispositifs médicaux numériques, le DMP, *etc*. présentent des risques élevés et doivent faire l'objet de mesures spécifiques.

A. Cloisonnement réseau et chiffrement des flux

85. Afin de limiter la propagation des logiciels malveillants, dont les rançongiciels (« cryptolockers ») qui bloquent les DPI des établissements de santé, et de freiner les attaques ciblées qui pénètrent par un système vulnérable et « rebondissent » vers le DPI, **la CNIL recommande de mettre en œuvre un cloisonnement réseau séparant strictement les flux réseaux propres au DPI**.

86. Ainsi, l'émission et la réception de flux de données internes au DPI seront restreintes, par des mesures spécifiques de filtrage réseau, aux seuls serveurs identifiés comme nécessaires au fonctionnement du DPI. De même, les flux externes seront restreints aux seuls serveurs identifiés comme chargés des échanges de données entre le DPI et les autres systèmes d'informations.

87. En outre, **la CNIL recommande que toutes les transmissions de données depuis ou vers le DPI,** ainsi que tous les flux de données internes entre les briques techniques du DPI**, fassent l'objet de mesures de chiffrement** conformes au référentiel général de sécurité[33] et aux recommandations de l'ANSSI[34] afin d'en garantir la confidentialité.

88. En particulier, **les canaux de communication** avec des systèmes externalisés, notamment ceux hébergés dans un système d'informatique en nuage (*Cloud)*, devraient être chiffrés et faire l'objet d'une **authentification mutuelle entre machines**, par certificat ou dispositif d'authentification équivalent[35].

B. Sécurisation des interfaces d'échanges de données (API)

Problème constaté :

Des images médicales de patients sont rendues librement accessibles via Internet par un logiciel d'imagerie mal configuré, dont l'interface DICOM[1] est activée par défaut, sans mot de passe.

89. Afin de limiter les risques liés aux échanges de données entre le DPI et d'autres applications, **la CNIL recommande que les interfaces (API) soient sécurisées par une authentification mutuelle forte** entre machines, assortie de profils d'accès spécifiques limités aux seules données nécessaires à chacune[36].

90. En particulier, le serveur dédié à la centralisation et au partage des fichiers issus de l'imagerie médicale (PACS) présente des vulnérabilités du fait des métadonnées identifiantes inscrites dans les fichiers (norme DICOM) et de ses interfaces de communication (API DICOM). Ces dernières doivent dès lors être verrouillées pour ne permettre d'accès qu'à travers les systèmes de l'établissement, en excluant tout accès direct au serveur DICOM depuis Internet.

91. En cas d'export des fichiers d'imagerie pour réutilisation à des fins de recherche ou d'entraînement d'un système d'intelligence artificielle, les métadonnées DICOM doivent être préalablement minimisées voire supprimées afin de réduire les risques de réidentification des patients. De la même manière, les cartouches de métadonnées incrustés visiblement dans les images doivent être minimisés, voire occultés, et les images contenant des éléments identifiables (par exemple, un tatouage, une prothèse, un implant dentaire, un pacemaker) doivent être floutées ou exclues si elles ne sont pas strictement nécessaires à la réalisation du projet.

[33] « RGS », ANSSI : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents
[34] « Mécanismes cryptographiques », ANSSI : https://cyber.gouv.fr/publications/mecanismes-cryptographiques
[35] Un mot de passe seul n'est pas considéré comme équivalent à un certificat.
[36] Voir la recommandation technique relative au partage de données par API, CNIL : https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-technique-relative-au-partage-de-donnees-par-api

Fiche 10 : l'information des personnes concernées

A. La distinction entre l'information RGPD et les informations « santé »

92. **Il convient de distinguer le droit des personnes à être informées des traitements de données à caractère personnel les concernant prévus par le RGPD et la loi « informatique et liberté » de celui prévu par des dispositions nationales** (code de la santé publique, code civil, *etc.*).

93. A titre d'exemple, le droit des personnes à être informées sur leur état de santé (article L. 1111-2 du CSP), sur les frais auxquels elles pourraient être exposées (L. 1111-3 du CSP) ou l'information relative à une recherche impliquant la personne humaine (L. 1122-1 du CSP) ne constitue pas une information concernant un traitement de données à caractère personnel.

94. Ces différentes informations peuvent être rassemblées au sein d'un document unique. Dans ce cas il est nécessaire que :

- la personne concernée puisse identifier facilement les renseignements relatifs à la mise en œuvre d'un traitement de données à caractère personnel ;
- l'information délivrée soit conforme aux dispositions du RGPD et de la loi « informatique et libertés ».

B. Droit des personnes à être informées et obligation de transparence du responsable de traitement

95. En application des articles 12, 13 et 14 du RGPD, **toute personne dispose d'un droit à être individuellement informée** des traitements de données à caractère personnel la concernant. De ce droit découle certaines obligations à la charge du responsable de traitement.

96. La commission des usagers, les associations des patients, les instances représentantes du personnel de l'établissement et les comités d'éthique pourraient être associés aux réflexions relatives à la forme et au fond de l'information délivrée aux personnes concernées.

1. Information au titre du DPI : rappels généraux

c. Qui est destinataire de l'information ?

97. Toute personne dont les données sont contenues dans un DPI (patient, professionnel de santé, tiers) doit être individuellement informée du traitement de ses données à caractère personnel[37].

98. **S'agissant des personnes majeures faisant l'objet d'une mesure de protection** (tutelle, curatelle, habilitation familiale ou mandat de protection future), la personne chargée d'une mission de représentation doit être informée du traitement de données à caractère personnel de la personne représentée. Dès lors que la personne majeure protégée est en état de prendre seule des décisions éclairées, celle-ci devrait être directement informée.

99. **S'agissant des personnes mineures**, les titulaires de l'autorité parentale doivent être informés du traitement de données à caractère personnel des personnes mineures dont ils ont la charge. La règlementation reconnaissant aux personnes mineures le droit de solliciter le secret de certaines informations le concernant vis-à-vis de ses représentants légaux[38], la CNIL estime que, dans ces hypothèses, seule la personne mineure doit être informée du traitement de ses données à caractère personnel. En toute état de cause, les titulaires de l'autorité parentale devront être informés du traitement de données à caractère personnel d'une personne mineure dont ils ont la charge dans le cadre :

[37] Cour de justice de l'Union européenne, affaire C-154/21, 12 janvier 2023 : qui consacre que le droit d'accès permet à la personne concernée de demander au responsable du traitement qu'il lui communique l'identité des destinataires auxquelles des données sont communiquées (et pas seulement les catégories de destinataires).

[38] Voir notamment les articles L. 1111-5, L. 1111-5-1, L. 2212-7 et L. 6211-3-1 du CSP

- d'une prise en charge précédente sans lien avec l'épisode de soin pour lequel la personne mineure demande le secret ;
- d'une prise en charge ultérieure sans lien avec l'épisode de soin pour lequel la personne mineure demande le secret.

d. Quelles sont les caractéristiques de l'information ?

100. L'information délivrée aux personnes ou à ses représentants légaux doit être :
    - réalisée au moment du recueil des données ;
    - facile d'accès ;
    - fournie gratuitement ;
    - fournie de manière claire et compréhensible ;
    - fournie de manière concise ;
    - distinguée des informations qui ne sont pas spécifiquement liées à la vie privée.

101. Cette information doit comporter l'ensemble des mentions prévues à l'article 13 ou, le cas échéant, 14 du RGPD. Il devra être indiqué que le droit d'opposition, le droit à la portabilité et le droit à l'effacement des données ne sont pas applicables. Le responsable de traitement pourra utilement rappeler que des mesures peuvent être mises en œuvre afin de restreindre l'accès à l'identité réelle du patient (par exemple, pour protéger la vie privée d'une personnalité publique, d'un patient dont des proches exercent dans l'établissement ; voir la Fiche 13 – Partie B), ainsi que les modalités pour en bénéficier.

102. De plus, des mentions spécifiques peuvent être requises au regard de certaines réglementations sectorielles (par exemple le recours à un prestataire d'hébergement externalisé[39]).

e. Comment déterminer le caractère adéquat de l'information ?

103. La CNIL recommande que l'information des personnes et ses modalités de délivrance soient pensées par l'établissement dès la conception du traitement et **tout au long du cycle de vie du DPI**.

104. Cette réflexion suppose de mener des analyses portant notamment sur :
    - les caractéristiques de la patientèle susceptible d'être prise en charge (établissement se trouvant à proximité d'une frontière, établissement spécialisé dans une catégorie de soins, établissement prenant en charge des personnes atteintes d'un handicap, *etc.*) ;
    - les catégories de personnes concernées par le traitement (patients mineurs, patients majeurs, proches du patient, professionnels participant à la prise en charge, *etc.*) ;
    - le contexte dans lequel se trouve l'établissement et des moyens dont il dispose (établissement privé, établissement public, existence d'une application ou plateforme d'échange entre le patient et l'établissement, *etc.*) ;
    - les spécificités applicables à certains services de soins (service des urgences, service de pédiatrie, *etc.*).

105. **Ces analyses permettront de déterminer les méthodes les plus adaptées pour délivrer l'information, la hiérarchie des informations à fournir**, *etc.* En outre, la documentation de cette approche, notamment dans l'AIPD, permettra au responsable de traitement de démontrer qu'il répond à ses obligations en matière de transparence.

106. Une réflexion en continu permet, d'une part, de s'assurer que les mesures initialement mises en œuvre remplissent les objectifs fixés et, d'autre part, d'identifier les mesures complémentaires à déployer afin de tenir compte de l'évolution du contexte dans lequel s'inscrit le traitement (déploiement de nouvelles technologies de communication, évolution du cadre juridique applicable).

[39] Article L. 1111-8 du CSP.

2. Information au titre des traitements ultérieurs

a. Qu'est-ce qu'un traitement de données ultérieur dans le cadre du DPI ?

107. Il est possible que les données à caractère personnel traitées au sein du DPI (traitement initial) soient réutilisées dans le cadre de traitements ultérieurs. Il peut, par exemple, s'agir de la réutilisation de données dans le cadre de la gestion des vigilances sanitaires, d'une recherche médicale, de la constitution d'un entrepôt de données de santé, de l'analyse de l'activité médicale, *etc.*

108. Ces traitements ultérieurs peuvent être mis en œuvre par l'établissement au sein duquel la personne a été prise en charge ou par un tiers (par exemple un industriel de santé, un institut de recherche) en qualité de responsable de traitement indépendant, ou conjointement entre le responsable du traitement initial et un tiers.

109. Ces **réutilisations et les traitements de données liés constituent des traitements distincts du DPI** auxquels l'ensemble des principes posés par le RGPD et la loi « informatique et libertés » sont applicables.

b. Quelles sont les obligations du responsable du traitement initial et du responsable de traitement ultérieur ?

110. Préalablement à toute réutilisation, **le responsable de traitement initial sera tenu d'évaluer la compatibilité de la finalité ultérieure par rapport à la finalité du DPI**. Pour réaliser ce test de compatibilité, le responsable du traitement initial devra tenir compte des éléments mentionnés à l'article 6.4 du RGPD, ainsi que de toute autre élément de nature avoir un impact sur les attentes légitimes des personnes concernées. L'utilisation de données de santé pseudonymisées à des fins de recherche est en principe compatible avec la finalité initiale de leur traitement.

111. Lorsque le traitement ultérieur est mis en œuvre par le responsable du traitement initial ou par le personnel exerçant sous sa responsabilité (l'établissement au sein duquel la personne a été prise en charge), **il sera tenu de fournir certaines informations à la personne concernée** (articles 13.3 et 14.4 du RGPD).

112. Lorsque le traitement ultérieur est mis en œuvre par un ou plusieurs responsables de traitement, distincts du responsable de traitement initial, l'obligation d'information et de transparence incombera à ce tiers. **Le responsable de traitement ultérieur sera tenu de fournir à la personne l'ensemble des informations requises par les articles 13 ou 14 du RGPD**. L'information réalisée par le responsable initial ne permettra pas de considérer que le responsable ultérieur a répondu à ses obligations.

113. La CNIL a pu remarquer que les données du DPI sont fréquemment réutilisées, notamment dans le cadre de projet de recherche ou pour la constitution d'entrepôt de données de santé. **Les établissements de santé sont invités à anticiper les modalités d'information des personnes dans le cadre de ces réutilisations** et à informer les personnes que leurs données pourront être réutilisées.

114. Cette information générale sur la réutilisation de ses données permet à la personne concernée d'avoir conscience que ses données feront l'objet d'un traitement pour une finalité différente de celle poursuivie lors de leur collecte (prise en charge). Le responsable du traitement ultérieur peut soit ;

- fournir une note d'information relative à chaque traitement ultérieur comportant l'ensemble des mentions prévues aux articles 13 et, le cas échéant 14 du RGPD ;
- recourir à une information « par paliers ».

115. Conformément au RGPD, lu à la lumière des lignes directrices sur la transparence du Comité européen de la protection des données CEPD[40], **le premier niveau d'une information « par paliers »** doit comporter les mentions suivantes :

- les catégories de finalité(s) poursuivies (par exemple à des fins de recherche, à des fins de constitution d'un entrepôt de données de santé) ;
- l'existence de droits pour la personne ;
- pour les traitement mis en œuvre à des fins de recherche, étude ou évaluation, les catégories d'organismes susceptibles de mettre en œuvre ces traitements ultérieurs (par exemple le personnel de l'établissement de prise en charge, des sociétés privées) ;

[40] JUSTICE AND CONSUMERS ARTICLE 29 - Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) (europa.eu)

- pour les traitements ne poursuivant pas une finalité de recherche (par exemple la constitution d'un entrepôt de données de santé), le ou les responsable(s) de traitement(s) ultérieur(s) ;
- le renvoi vers un portail de transparence, ou dispositif équivalent de transparence, sur lequel sera publié une note d'information comportant l'ensemble des informations requises par l'article 13 du RGPD, ou le cas échéant l'article 14 du RGPD.

116. La CNIL recommande, par ailleurs, que cette information soit complétée des mentions suivantes :
    - l'existence d'un droit d'opposition à la réutilisation de ses données (si applicable) ;
    - le fait que l'exercice de ses droits, notamment son droit d'opposition, n'aura aucune incidence sur sa prise en charge sanitaire.
117. Toute autre information jugée pertinente par le responsable de traitement ou qui serait susceptible d'avoir une incidence importante pour la personne concernée par le traitement initial pourra être ajoutée sur cette mention d'information.

C. Les recommandations pour l'information des patients

Problèmes constatés :

- Les notes d'information ne contiennent pas l'ensemble des mentions prévues par l'article 13 du RGPD.
- Les notes d'information sont uniquement accessibles sur des supports dématérialisés.
- Le premier niveau d'information de la personne ne renvoie pas vers la note d'information comprenant l'ensemble des mentions prévues par l'article 13 du RPGD.
- L'information RGPD est incluse dans un document d'information plus général.

1. Information au moment du recueil des données

118. Dès lors que les données sont collectées directement auprès du patient, **l'information doit lui être délivrée**, ou à ses représentants légaux, **dès l'obtention des données**, sauf si elle en a déjà connaissance.
119. La CNIL recommande que le patient ou ses représentants légaux soient informés :
    - dès la première prise de rendez-vous ; **et**
    - lors de l'accueil pour la prise en charge quelle qu'en soit les modalités.
120. Dans l'hypothèse où le patient serait inconscient lors de son admission dans l'établissement, l'information devra lui être délivrée dès que son état de santé le permet. Dans l'attente, il est recommandé d'informer les proches du patient présents.
121. Afin de déterminer si le patient dispose déjà des informations relatives à la mise en œuvre d'un traitement de données à caractère personnel, il est recommandé de :
    - **formaliser une procédure** relative aux documents d'information à remettre à la personne ;
    - **tracer cette remise**.

2. Information facile d'accès

122. L'exigence d'accessibilité de l'information signifie que **la personne ne devrait ni avoir à demander l'information, ni à la rechercher, ni rencontrer des difficultés pour la trouver**. Il appartient à l'établissement de santé de prendre les mesures nécessaires pour fournir l'information ou diriger activement la personne vers l'endroit où elle peut la trouver.
123. Lors de sa prise en charge sanitaire, la personne reçoit de nombreux documents et informations (sur son état de santé, sur les démarches à mener, *etc.*). Ainsi, il est recommandé de **multiplier les canaux de diffusion de l'information relative au traitement de ses données, de façon à garantir sa visibilité et son appropriation par la personne**.

124. La CNIL recommande que la note d'information soit cumulativement :

- envoyée par courrier électronique à la personne concernée sous réserve de respecter les mesures de sécurité décrites dans la Fiche 11 ;
- insérée dans le livret d'accueil mentionné à l'article L. 1112-2 du CSP ;
- affichée dans les lieux d'accueil du public de l'établissement ;
- diffusée sur le site web de l'établissement et accessible dès la page d'accueil.

125. Ces modalités d'information écrites pourraient être utilement complétées, à titre d'exemple, par de vidéos, animations, dessins animés ou bandes dessinées disponibles ou diffusés dans les lieux d'accueil du public.

126. **Les autres documents remis au patient** (compte-rendu, résultat d'analyse, *etc.*) pourront utilement comporter une mention relative au traitement de données à caractère personnel mis en œuvre dans le cadre de leur prise en charge renvoyant aux autres supports d'information (affichage ou diffusion sur site web).

3. Information claire et compréhensible

127. L'information doit être **rédigée de la manière la plus claire, précise et simple possible**.

128. Cela implique notamment les mesures suivantes :

- utiliser un vocabulaire simple (éviter les termes juridiques ou techniques). La CNIL propose des exemples de termes simplifiés sur son site web ;
- faire des phrases courtes et employer un style direct (éviter les termes imprécis ou, ambigus et les formules telles que « une possible utilisation de vos données », « quelques données vous concernant sont utilisées », *etc.*) ;
- adapter l'information au public visé. Les établissements de santé sont également invités à déterminer si d'autres mesures pourraient être mises en œuvre comme, par exemple, la traduction des supports d'information dans une autre langue ou l'adoption de la méthode FALC (Facile à lire et à comprendre).

129. **S'agissant des personnes mineures**, la CNIL recommande qu'une information leur soit délivrée, en fonction de leur capacité de discernement et de compréhension et *a minima* aux mineurs âgés de quinze ans ou plus[41].

130. **S'agissant des personnes majeures faisant l'objet d'une mesure de protection juridique** (curatelle, tutelle, sauvegarde justice), la CNIL recommande qu'elles soient systématiquement informées, en fonction de leur capacité de compréhension et de discernement.

4. Information concise

131. Cette exigence suppose que l'établissement de santé présente les informations d'une manière efficace et succincte.

132. À cet égard, il est possible **d'adopter une logique d'information « par paliers »**. Cette approche « par paliers » suppose de prendre en compte l'inégalité d'accès de la population aux nouvelles technologies et à Internet.

133. Dès lors qu'une logique d'information « par paliers » est adoptée, le premier niveau d'information devrait *a minima* comporter les informations suivantes :

- **l'identité du responsable de traitement** ;
- la **finalité** poursuivie ;
- **l'existence de droits** et la manière de les exercer ;
- un **renvoi vers l'endroit où peut être consultée la note d'information complète** (politique de confidentialité d'un site web, affichage dans les lieux accessibles au public). Ce renvoi doit être direct et explicite.

[41] Pour plus d'informations sur les droits numériques des mineurs : « Les droits numériques des mineurs », CNIL : https://www.cnil.fr/fr/thematiques/les-droits-numeriques-des-mineurs

134. S'agissant du livret d'accueil, celui-ci devra, outre les éléments mentionnés ci-dessus, comporter les informations prévues à l'article R. 1112-9 du CSP.

5. Information spécifique à la vie privée

135. Le droit à l'information consacré par le RGPD **ne doit pas être confondu avec les autres droits à l'information reconnus au patient dans le secteur de la santé**.

136. La CNIL recommande que l'information au titre d'un traitement de données à caractère personnel soit, dans la mesure du possible, physiquement et logiquement séparée des autres catégories d'information.

137. La CNIL recommande cumulativement les pratiques suivantes :

- **s'agissant du livret d'accueil**, une partie devrait être dédiée à l'information concernant le traitement de données lié au DPI ;
- **s'agissant de l'affichage dans les lieux accessibles au public**, l'information concernant le traitement de données lié au DPI devrait être distinguée des supports d'information traitant de sujets différents (par exemple, information sur des modalités de prise en charge, sur des campagnes de dépistages ou sur la réalisation de recherches) ;
- **s'agissant de la diffusion sur le site web de l'établissement**, l'information concernant le traitement de données lié au DPI devrait faire l'objet d'un onglet dédié accessible dès la page d'accueil du site web ;
- **s'agissant des mentions figurant sur les autres documents remis au patient**, l'information concernant le traitement de données lié au DPI devrait être physiquement et graphiquement distinguée des autres informations contenues dans le document.

6. Information sur des traitements ultérieurs

138. Les traitements ultérieurs procédant à la réutilisation des données traitées dans le cadre du DPI constituent des traitements distincts qui doivent faire l'objet de mesures d'information dédiées. **L'information individuelle des patients concernant chaque traitement ultérieur est en principe requise** en application des articles 13 et, le cas échéant 14 du RGPD, ainsi que les articles 69 et suivants de la loi « informatique et libertés ». Des dérogations peuvent être appliquées dès lors que les conditions posées par l'article 13.4 et 14.5 du RGPD sont remplies.

139. Il convient de bien distinguer la présentation des mentions d'information afin que la personne puisse aisément comprendre :

- le caractère ultérieur de ce second traitement (réutilisation) ;
- ses caractéristiques essentielles : identité du responsable de traitement, finalité, durées de conservation, *etc.* ;
- les droits dont elle dispose concernant ce traitement ultérieur.

140. Aussi, la CNIL recommande aux établissements de santé :

- de mener une réflexion afin de **cartographier les catégories de traitements ultérieurs** susceptibles d'être menés et leurs caractéristiques essentielles ;
- **d'anticiper les modalités d'information** qui pourraient être mobilisées afin de satisfaire à leurs obligations.

141. Par exemple dans le cadre de la réutilisation des données du DPI à des fins de recherche, les mesures suivantes peuvent être envisagées (liste non limitative) :

- une mention d'information générique sur la réutilisation des données à des fins de recherche inscrite sur le livret d'accueil, affichée dans les lieux accessibles au public et précisant l'endroit ou la personne auprès de laquelle des informations plus détaillées sur ces réutilisations peuvent être consultées ;
- la création d'une page web dédiée listant l'ensemble des recherches menées à partir des données collectées dans le DPI (portail de transparence) ;
- publicité de la création du portail de transparence (publication sur un journal local).

142. La CNIL recommande qu'un moteur de recherche permettant d'ajouter des filtres soit mis en œuvre sur le portail de transparence.

D. Les recommandations pour l'information des proches du patient

143. Des données à caractère personnel relatives à des proches, peuvent, et dans certains cas doivent, être traitées dans le cadre du DPI. Il s'agit par exemple de la personne de confiance, la personne à prévenir, des représentants légaux du patient, des membres de la famille (notamment dans le cadre de la collecte des antécédents médicaux). **Ces personnes disposent également d'un droit à être informées du traitement de leurs données**. Cette information et ces modalités de délivrance doivent être adaptées à chaque catégorie de personnes concernées et ne doivent pas porter atteinte au secret professionnel.

144. Les grands principes développés ci-dessus (Partie B) ainsi que leur traduction pratique (Partie C) sont applicables à l'information des proches avec les particularités suivantes.

1. Les proches dont les données directement identifiantes et les coordonnées sont collectées

145. Il s'agit notamment de la personne de confiance, la personne à prévenir, des représentants légaux ainsi que des titulaires de l'autorité parentale.

146. **S'agissant des données à caractère personnel directement collectées auprès de ces personnes (proches présents lors de l'accueil du patient)**, ceux-ci devraient être **individuellement informés** dans les mêmes conditions que le patient sauf s'ils l'ont déjà été.

147. **S'agissant des données collectées par l'intermédiaire du patient (collecte indirecte par exemple par le biais d'un formulaire rempli par le patient)**, au regard du nombre de patients transitant en établissement de santé par jour et conformément aux lignes directrices relatives à la transparence du CEPD (§62), l'information individuelle de ces personnes exigerait des efforts disproportionnés au sens de l'article 14.5.b) du RGPD.

148. Dans cette hypothèse, le responsable de traitement est tenu de **prendre les mesures appropriées afin de rendre les informations publiquement disponibles**. Ces mesures peuvent notamment prendre la forme d'une diffusion sur son site web de l'information concernant le traitement de données lié au DPI. Cette information devrait faire l'objet d'un onglet dédié accessible dès la page d'accueil du site web et comprendre l'ensemble des mentions prévues par l'article 14 du RGPD.

2. Les proches dont les données directement identifiantes et les coordonnées ne sont pas collectées

149. Dans le cadre de la prise en charge, la collecte des antécédents médicaux peut conduire à celles de donnée à caractère personnel des membres de la famille du patient.

150. Les finalités pour lesquelles ces données sont collectées n'imposent pas au responsable de traitement d'identifier la personne tierce concernée. Aussi, en application de l'article 11 du RGPD, **le responsable de traitement n'est pas tenu d'obtenir ou de traiter des informations supplémentaires pour l'identifier ou pour l'informer du traitement de ces données à caractère personnel**.

151. La CNIL recommande néanmoins que le responsable de traitement **diffuse sur son site web l'information concernant le traitement de données lié au DPI** en précisant qu'il est susceptible de porter sur des données indirectement identifiantes des membres de la famille des patients.

E. Les recommandations pour l'information des professionnels participant à la prise en charge

152. Des données à caractère personnel concernant les professionnels intervenant dans la prise en charge de la personne peuvent, et dans certains cas doivent, être traitées dans le cadre du DPI. **Ces professionnels disposent d'un droit à être informés du traitement de leurs données.**

153. Les grands principes développés ci-dessus (Partie B) ainsi que leur traduction pratique (Partie C) sont applicables à l'information des professionnels, avec les particularités suivantes.

1. Le personnel de l'établissement de santé

Problèmes constatés :

- Les notes d'information ne contiennent pas l'ensemble des mentions prévues par l'article 13 du RGPD.
- Le premier niveau d'information de la personne ne renvoie pas vers la note d'information comprenant l'ensemble des mentions prévues par l'article 13 du RPGD.

154. La CNIL recommande que ces personnes soient informées **dès leur embauche** par la remise d'une notice dédiée au traitement lié à la mise en œuvre du DPI. Cette notice peut être intégré aux documents remis aux nouveaux arrivants dans l'établissement.

155. Cette notice peut également être **distinguée des autres supports d'information relatifs à d'autres traitements** de données à caractère personnel que l'établissement met en œuvre (par exemple, traitement de données à des fins de gestion de la paie).

156. Dès lors que les données relatives au personnel de l'établissement traitées dans le cadre du DPI sont réutilisées dans le cadre de traitements ultérieurs, la CNIL recommande qu'un premier niveau d'information comportant l'ensemble des mentions précisées ci-dessus (VII.B.6) leur soit délivré.

2. Les professionnels de santé externes à l'établissement de santé

157. **S'agissant des cas dans lesquels les données sont collectées directement auprès de professionnels extérieurs**, ceux-ci devraient être **destinataires en retour d'une notice d'information dédiée** au traitement de leurs données à caractère personnel.

158. **S'agissant des cas dans lesquels les données sont collectées indirectement auprès des professionnels (par exemple fourniture par le patient d'un compte-rendu de biologie médicale réalisé en ville)**, il convient de déterminer si leur information peut être réalisée via des échanges ultérieurs notamment par l'intermédiaire du patient (par exemple lors de la remise de la fiche de liaison). Dans cette hypothèse, **l'information individuelle des professionnels** est requise.

159. Dans l'hypothèse où aucun échange ultérieur n'interviendrait et au regard du nombre de documents pouvant être remis à un établissement de santé par jour, l'information individuelle de ces professionnels exigerait des efforts disproportionnés de la part du responsable de traitement au sens de l'article 14.5.b) du RGPD. Le responsable de traitement reste tenu de prendre les mesures appropriées afin de rendre les informations publiquement disponibles. La CNIL recommande de **mettre en place un dispositif de transparence dédié à l'information des professionnels externes** à l'établissement de santé. Ce dispositif pourrait être mis en œuvre sur le site web du responsable de traitement dans une page dédiée.

Fiche 11 : les mesures de sécurité liées à l'information et l'exercice des droits

160. **L'envoi au patient d'une note d'information par messagerie électronique est susceptible de révéler à ses proches ou à des tiers des informations sur sa santé qui sont couvertes par le secret professionnel** (par exemple, si l'envoi provient d'un centre de prise en charge du cancer). Cette opération doit se faire dans le respect du secret professionnel.

161. Des modalités spécifiques peuvent être mises en œuvre, par exemple :

- utiliser une messagerie sécurisée de santé constituant un espace de confiance partagé entre professionnels de santé et patients (par exemple, la « MSSanté » en lien avec « MonEspaceSanté ») ;
- mettre en place des mesures de sécurité protégeant la note d'information (par exemple, pièce jointe chiffrée ou lien de téléchargement protégé par mot de passe, le code étant transmis par texto) ;
- s'assurer que ni la note d'information ni son expéditeur ne donne d'information sur l'état de santé des personnes.

162. En cas de demande d'accès, la CNIL recommande de **privilégier la remise en main propre au patient de son dossier médical** car elle permet de vérifier son identité avec une meilleure fiabilité. En cas de transmission du dossier médical par courrier, il est recommandé de le réaliser sous enveloppe scellée conçue pour révéler une tentative d'ouverture, avec remise en main propre par le facteur et accusé de réception (LRAR).

163. **En cas de transmission du dossier médical par voie électronique**, la CNIL recommande l'utilisation d'une plateforme sécurisée imposant une authentification multifacteur, mise en place après vérification de l'identité du destinataire et recueil auprès de lui de ses facteurs d'authentification (par exemple, un mot de passe et un numéro de téléphone mobile).

164. Lorsqu'une telle solution ne peut être mise en œuvre ou en cas de refus par le patient d'y recourir, la CNIL recommande que l'envoi se fasse par messagerie électronique dans une pièce jointe chiffrée dont le code de déchiffrement sera transmis par un autre canal, préalablement recueilli et vérifié (courrier postal, téléphone, texto, etc.).

165. Si le patient exige un envoi par messagerie électronique en clair, l'établissement devra avertir l'intéressé des risques que présente cet envoi ; **la CNIL recommande alors de lui faire signer un document indiquant qu'il a été informé des risques et a refusé les solutions sécurisées proposées par l'établissement.**

Fiche 12 : le personnel du responsable de traitement

A. Le personnel du responsable de traitement

166. Le responsable de traitement est tenu de mettre en place les mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est respectueux de la vie privée des personnes concernées et garantit la protection des données traitées. Ces mesures doivent notamment garantir que les personnes agissant sous l'autorité directe du responsable de traitement et celle de ses sous-traitants ne traitent ou n'accèdent qu'aux données nécessaires à l'exercice de leurs fonctions et que sur instruction du responsable de traitement[42].

167. Dans le cadre du DPI, ces principes doivent également s'articuler avec le secret professionnel et la notion d'équipe de soins. Les professionnels de santé sont tenus à une obligation de secret[43]. Cette obligation s'applique également à tout professionnel intervenant dans le système de santé quel que soit sa compétence, son statut et le fait qu'il ait ou non accès aux dossiers des patients[44] (personnel administratif, secrétaire médical, assistant social, éducateur spécialisé, etc.).

168. Dans certains cas, il peut être nécessaire de restreindre les accès des personnes pouvant accéder à l'identité réelle d'un patient, indépendamment de la notion d'équipe de soins. Il peut s'agir d'une confidentialité simple, c'est-à-dire la non divulgation de la présence du patient[45] à sa demande ou d'une confidentialité renforcée, par exemple dans les cas où les proches du patient exercent dans la structure de santé où il est soigné ou encore si le patient est reconnu comme une personnalité publique[46] (voir la Fiche 13 – Partie B).

1. Les membres de l'équipe de soins

169. La notion **d'équipe de soins** est fondamentale car elle détermine quel professionnel a le droit d'accéder au DPI d'un patient, quelles sont les données à caractère personnel auxquelles il peut accéder ainsi que les conditions dans lesquelles l'échange et le partage de ces données est possible.

a. Définition de l'équipe de soins

170. La notion d'équipe de soins est définie comme l'ensemble des professionnels participant à la prise en charge d'un même patient et effectuant à ce titre un acte diagnostique, thérapeutique, de compensation du handicap, de soulagement de la douleur ou de prévention de perte d'autonomie, ou aux actions nécessaires à la coordination de plusieurs de ces actes[47]. Les professionnels concernés sont listés à l'article R. 1110-2 du CSP. L'équipe de soins n'est pas figée.

171. Le code de la santé publique distingue :

- **l'échange d'informations** entre professionnels relatives à une même personne prise en charge[48] à condition que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins de ladite personne ;
- **le partage d'informations** concernant une même personne[49] lorsque ces professionnels appartiennent à la même équipe de soins à condition que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins de la personne concernée.

172. Au sein de l'équipe de soins, l'échange et le partage de données à caractère personnel concernant le patient ne requièrent pas son consentement exprès. Il dispose néanmoins du droit de s'y opposer, et doit en être informé préalablement.

[42] Article 32, paragraphe 4 du Règlement général sur la protection des données.
[43] Article L. 1110-4 du code de la santé publique.
[44] Cour de Cassation, chambre sociale, 7 octobre 1997, 93-41.747.
[45] Article R. 1112-45 du code de la santé publique.
[46] Article R. 1112-45 du code de la santé publique.
[47] Article L. 1110-12 du code de la santé publique.
[48] Article L. 1110-4 du code de la santé publique (II)
[49] Article L. 1110-4 du code de la santé publique (III)

173. Pour être qualifiés de membres de l'équipe de soins, ces professionnels doivent soit[50] :

- exercer au sein du même établissement de santé[51] (et intervenir dans la prise en charge du patient) ;
- s'être vus reconnaître cette qualité par le patient lui-même (dans cette hypothèse, la qualité de membre de l'équipe de soins ne peut pas être présumée et suppose un acte positif du patient par exemple la prise d'un rendez-vous en vue de la réalisation d'une consultation ou de la réalisation d'un acte médical suite à la prescription par un médecin) ;
- appartenir à un ensemble de professionnels intervenant dans la prise en charge d'un même patient dès lors qu'au moins un de ces professionnels est un professionnel de santé[52].

b. Quelles données les membres d'une équipe de soins peuvent-ils échanger et partager ?

174. Les professionnels relevant de l'équipe de soins peuvent échanger et partager des données à caractère personnel relatives à un patient sous réserve :

- qu'ils participent à sa prise en charge médicale, sociale ou médico-sociale et qu'ils effectuent à ce titre différents actes tels que mentionnés ci-dessus ;
- que les données concernées soient strictement nécessaires à sa prise en charge, ce qui est défini par leurs attributions (métier) dans la matrice d'habilitation[53].

175. Seules les informations utiles à la prise en charge globale peuvent être échangées ou partagées.

176. Pour créer des profils d'habilitation selon les métiers[54], le responsable de traitement doit :

- procéder à un état de lieux des différents profils exerçant au sein de l'établissement ;
- se doter d'une matrice d'habilitation définissant les règles d'accès au DPI et les données à caractère personnel consultables par défaut par les professionnels en fonction des profils identifiés. La matrice d'habilitation doit également définir les règles d'accès pour chaque service de l'établissement (voir la Fiche 13 – Partie B) ;
- identifier individuellement chaque professionnel concerné et garantir qu'il s'agit de la bonne personne (voir la Fiche 13 – Partie A) ;
- prévoir des habilitations spécifiques (voir la Fiche 13 – Partie B).

177. La matrice d'habilitation est conçue et maintenue à jour par un comité de gouvernance. Elle doit tenir compte des évolutions portant sur le champ de compétence et/ou la pratique de soin de ces professionnels, qu'ils soient des professionnels de santé ou non. Il est recommandé qu'elle soit soumise à l'avis de la commission médicale d'établissement.

2. Le personnel ne relevant pas de l'équipe de soins et pouvant avoir accès à certaines données du DPI

178. Des professionnels, salariés de l'établissement, peuvent être amenés à accéder au DPI alors qu'ils ne participent pas à la prise en charge de la personne concernée. Cet accès peut être :

- imposé par la règlementation applicable, c'est notamment le cas des médecins responsables de l'information médicale (médecin DIM) ;
- justifié par les besoins des autres traitements mis en œuvre par le responsable de traitement. Il est, par exemple, admis que les attachés de recherche clinique (ARC) et les techniciens d'études cliniques (TEC) de l'établissement aient accès, en lecture, au DPI des patients inclus dans l'étude afin de vérifier les données à caractère personnel transmises et remplir le CRF.

[50] Article L. 1110-12 du code de la santé publique.
[51] Plusieurs structures sont directement visées à l'article L. 1110-12 du code de la santé publique et l'article D. 1110-3-4 liste les structures de coopération, d'exercice partagé ou de coordination sanitaire ou médico-sociale dans lesquelles peuvent exercer les membres d'une équipe de soins le (décret n°2016-996 du 20 juillet 2016).
[52] Arrêté du 25 novembre 2016 fixant le cahier des charges de définition de l'équipe de soins visée au 3° de l'article L. 1110-12 du code de la santé publique.
[53] Article R. 1110-1 du code de la santé publique.
[54] Voir en ce sens la décision n° MED-2023-074, citée dans les Tables Informatique et Libertés de la CNIL.

179. Dans tous les cas, ces salariés :

- doivent être spécialement habilités par le responsable de traitement (voir la Fiche 13 – Partie B) ;
- accèdent, sous la responsabilité du responsable de traitement, aux données strictement nécessaires à l'exercice de leurs missions, dans la limite de leurs attributions respectives.

180. En principe, le partage hors équipe de soins de données à caractère personnel couvertes par le secret professionnel nécessite de recueillir le consentement préalable du patient[55]. Ce consentement au partage de données à caractère personnel doit répondre aux conditions posées par les articles R. 1110- 3 et suivants du CSP.

181. Dans certaines hypothèses, limitativement prévues par les textes, ce partage peut intervenir après information du patient et sous réserve qu'il ne s'y oppose pas. C'est notamment le cas pour l'accès aux données du DPI par :

- le médecin DIM pour l'analyse de l'activité médicale de l'établissement[56] ;
- les personnes chargées du contrôle qualité d'une recherche impliquant la personne humaine[57]. Plus précisément, il s'agit des ARC et des TEC mandatés par le promoteur de la recherche.

[55] Article L. 1110-4 du code de la santé publique.
[56] Articles L. 6113-7, R. 6113-1 et R. 6113-7 du code de la santé publique.
[57] Article L. 11121-3 du code de la santé publique.

Fiche 13 : les mesures de sécurité liées aux accédants

A. Comptes utilisateurs et authentification multifacteur

Problèmes constatés :

- mots de passe de six caractères, non sensibles à la casse.
- mots de passe de moins de douze caractères sans mesure complémentaire (par ex. temporisation d'accès au compte après plusieurs échecs).
- pas de mécanisme de vérification automatique de la complexité des mots de passe lors de leur création.
- accès distant au DPI en authentification simple (nom d'utilisateur et mot de passe).
- compte utilisateur générique utilisé indifféremment par l'équipe technique d'un prestataire de maintenance.

182. Chaque utilisateur du DPI, et chaque personne amenée à accéder aux systèmes sur lesquels il repose, doit avoir un compte personnel basé sur un identifiant unique et nominatif. Cela permet notamment d'assurer la traçabilité des accès au DPI et des modifications de données (voir la Partie C).

183. Par exception, dans le cas d'équipements techniques ne gérant pas plusieurs comptes utilisateurs, des comptes génériques peuvent être utilisés s'ils sont associés à des mesures permettant de tracer nominativement leur utilisation. La CNIL recommande alors, par exemple :

    - de les rendre uniquement accessibles à travers un bastion d'administration ;
    - ou de mettre en place une main courante, liée à une autorisation préalable de la hiérarchie et au renouvellement du mot de passe dès que la personne n'a plus besoin d'accéder au compte.

184. De manière générale, **une authentification multifacteur offre une protection bien supérieure au mot de passe seul**. Elle est recommandée pour sécuriser l'accès aux données personnelles sensibles et ainsi protéger leur confidentialité, leur intégrité et leur disponibilité. Elle est également nécessaire pour permettre une imputabilité à valeur probante des traces de journalisation du DPI (voir la Partie C).

185. Les référentiels d'identification de la Politique générale de sécurité des systèmes d'information en santé (PGSSI-S)[58] portent l'exigence depuis juin 2022 d'une authentification multifacteur pour tout accès externe à un système informatique de santé, que ce soit par un professionnel de santé ou un patient, et à partir de janvier 2026 pour tout accès interne à l'établissement. La CNIL avait eu l'occasion de rendre un avis sur ces référentiels, en insistant sur la nécessité de mettre en œuvre une authentification multifacteur pour tout accès interne, dans les meilleurs délais et « au plus tard » en 2026.

186. En effet, les moyens d'identification électronique dits « de transition », qui sont prévus par la PGSSI-S pour apporter un niveau de sécurité minimal dans l'attente d'une authentification multifacteur locale, ne doivent pas faire perdre de vue l'échéance de janvier 2026 et la nécessité de lancer au plus tôt les chantiers nécessaires à l'atteinte de la cible.

187. Dès lors, tout accès interne ou externe aux données du DPI devrait être subordonné à une authentification faisant intervenir *a minima* deux facteurs d'authentification distincts, et doit l'être à partir du 1er janvier 2026. Si un de ces facteurs est un mot de passe, celui-ci devrait être conforme aux recommandations de la CNIL en matière de mot de passe, dans leur dernière version publiée[59]. La mise en œuvre de ce mode d'authentification doit faire l'objet d'un accompagnement, d'un suivi et d'une sensibilisation régulière des utilisateurs, tant pour la prise en main des moyens d'authentification que pour leur paramétrage et leur utilisation quotidienne (mot de passe robuste, canal sécurisé strictement personnel, etc.).

[58] « PGSSI-S », ANS : https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

[59] À date, délibération n° 2022 100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés. « Mots de passe : une nouvelle recommandation pour maîtriser sa sécurité », CNIL : https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite

188. Afin de concilier les impératifs de sécurité et d'ergonomie pour les professionnels de santé en établissement, l'authentification multifacteur interne peut disposer d'une durée de session longue sans dépasser une demi-journée.

189. De même, **en cas d'indisponibilité d'un des facteurs d'authentification** (par exemple, oubli ou perte de la carte à puce ou du téléphone mobile, panne du réseau téléphonique, etc.), **un mode alternatif doit être prévu, avec un niveau de sécurité équivalent** (par exemple, remise d'une carte à puce de dépannage, tracée dans une main courante).

190. **Concernant les sous-traitants intervenant sur le DPI, les mêmes mesures s'appliquent**, notamment pour répondre à l'obligation de conserver leurs traces d'accès. Comme ces utilisateurs ne bénéficient pas de la CPS, des identifiants nominatifs et une authentification multifacteur locale doivent être mise en place. Il est également possible de recourir à des CPE de service non nominatives, à la condition que leur attribution soit systématiquement tracée dans une main courante, de même que leur restitution en fin de mission, qui devra être contrôlée.

B. Gestion des habilitations

Problèmes constatés :

- Des professionnels de l'établissement accèdent aux dossiers de patients sans participer directement à leur prise en charge, à la coordination ou à la continuité de leurs soins.
- Tous les utilisateurs du DPI peuvent rechercher n'importe quel patient et visualiser l'intégralité de son dossier.
- Le mode « bris de glace » nécessite uniquement la saisie d'une justification en champ libre, où un simple caractère espace (« ») suffit.
- Des professionnels qui ne sont plus habilités à accéder au DPI ont conservé leurs droits d'accès.
- Du personnel médical extérieur à l'établissement est habilité à accéder au DPI et peut y consulter l'ensemble des dossiers médicaux.
- Un simple appel téléphonique à l'administrateur système suffit pour obtenir une habilitation supplémentaire (par exemple, le rattachement à un nouveau service).

191. **Les données à caractère personnel d'un patient doivent être uniquement accessibles aux membres de son équipe de soins** (voir la Fiche 12 – Partie A.1).

192. Pour cela, **une politique de gestion des habilitations doit être définie et mise en œuvre**, en prenant en compte le type de métier, ou la fonction exercée, ainsi que la notion d'équipe de soins. **Les personnes autorisées à accéder au logiciel DPI doivent être individuellement habilitées**, selon une procédure formelle impliquant une validation par leur responsable hiérarchique.

193. **Différents profils d'habilitation, correspondants aux différents métiers, doivent être prévus afin de gérer et paramétrer les accès au DPI en tant que de besoin et de façon exclusive**, conformément à la politique définie[60].

194. À cet égard, si une « matrice d'habilitation » peut couvrir les aspects métiers, une gestion spécifique des habilitations est nécessaire concernant l'équipe de soins, en s'appuyant de préférence sur l'unité fonctionnelle, l'unité de soins, ou sinon le service, qui prend en charge le patient.

195. De plus, la granularité des accès associés aux profils d'habilitation doit tenir compte des **principes de cloisonnement des données** (données administratives, NIR, INS, données de santé structurées, documents textuels, imagerie, données génétiques – voir la Fiche 6). La CNIL recommande également de tenir compte d'autres **typologies particulières** (par exemple, données particulièrement sensibles relatives à la psychiatrie, au suicide, à la fertilité, à l'infectiologie d'urgence, à l'aide médicale d'état, au judiciaire, aux pratiques des professionnels de santé).

196. Enfin, il est de bonne pratique, quand la prise en charge du patient par un service donné s'achève, que **les personnels de ce service ne conservent pas l'accès** à son dossier au-delà du temps nécessaire pour finaliser leurs saisies (par exemple, quelques jours pour les infirmiers, un mois pour le secrétariat spécialisé pour les comptes rendus).

[60] Voir en ce sens la décision n° MED-2024-067.

197. Dans certains cas, **il peut être nécessaire ou souhaitable de restreindre les personnes pouvant accéder à l'identité réelle d'un patient** (par exemple, pour protéger la vie privée d'une personnalité publique, d'un patient dont des proches exercent dans l'établissement ; voir la Fiche 12 – Partie A). Dans un tel cas, la CNIL recommande de remplacer l'identité du patient concerné par un alias, qui sera seul visible pour les accès courants au dossier, ou en utilisant un mode « très confidentiel » permettant de restreindre l'accès du dossier à une équipe de soins spécialement désignée.

198. La règlementation prévoit certaines hypothèses dans lesquelles **un mineur peut solliciter le secret des informations le concernant** vis-à-vis de ses représentants légaux[61]. Afin de garantir la confidentialité des données à caractère personnel et des documents concernés par la demande de la personne mineure, le DPI devrait permettre **d'identifier spécifiquement ces données et ces documents** lors de leur saisie ou de leur importation par un professionnel. **Lors de leur consultation par un professionnel de santé, le DPI peut par exemple présenter une mention d'alerte spécifique** (par exemple : « Ne pas communiquer ces informations aux parents »). De même, ces données ou documents doivent être masqués lorsque le dossier d'un patient mineur est communiqué ou rendu accessible à un représentant légal du mineur concerné.

199. Afin de répondre aux situations d'urgence pour lesquelles un professionnel de santé doit intervenir alors qu'il n'est pas membre de l'équipe de soins du (ou des) patient(s) concerné(s), **une fonctionnalité d'accès de type « bris de glace » doit permettre l'attribution temporaire et exceptionnelle de droits d'accès en cas d'urgence ou de situation de crise**. Cette fonctionnalité doit impérativement assurer que ces accès sont tracés et justifiés, avec le nom de l'utilisateur et un motif issu d'une liste prédéfinie. Les droits attribués doivent être adaptés au motif déclaré (par ex. pour une recherche d'antécédents : simple liste de l'historique des séjours, et pour dispenser des soins en urgence : accès complet au séjour en cours).

200. Les accès privilégiés disposant de droits étendus, notamment pour l'administration et la maintenance, doivent être réservés à une équipe restreinte et être limités au strict nécessaire en termes de périmètre et de durée.

201. **La CNIL recommande de procéder chaque année à une revue manuelle ou automatique des habilitations**. Cette revue permet de vérifier que :

- les habilitations attribuées sont toujours justifiées ;
- la fin des accès temporaires et les retraits d'habilitation liés aux départs ou aux changements de fonction du personnel ont bien été pris en compte, et effectuer le cas échéant les mesures correctives nécessaires.

202. **Les permissions techniques d'accès au DPI doivent être supprimées ou mises à jour dès le retrait ou la modification d'une habilitation**, ainsi que lors du départ ou du changement de service d'une personne habilitée. Pour cela, l'établissement peut mettre en place une procédure d'information depuis le service des ressources humaines vers les administrateurs fonctionnels du DPI ou, encore mieux, un circuit automatisé depuis le système d'information des ressources humaines de l'établissement vers le système d'information hospitalier et le DPI.

[61] Voir notamment les articles L. 1111-5, L. 1111-5-1, L. 2212-7 et L. 6211-3-1 du CSP

C. Traçabilité

Problèmes constatés :

- le dossier patient de personnalités publiques hospitalisées est consulté par un nombre de professionnels dépassant largement leur équipe de soins ;
- le dossier patient de professionnels pris en charge dans leur établissement d'exercice est consulté par des collègues indiscrets ;
- le contrôle des traces d'accès au DPI n'est pas réalisé proactivement mais uniquement suite à des plaintes ;
- le contrôle de la légitimité des accès au DPI est réalisé manuellement et n'est pas documenté ;
- en l'absence de traçabilité précise des accès au DPI, il n'est pas possible d'identifier à quelles informations un utilisateur a accédé à l'intérieur d'un dossier médical, ce qui place l'établissement en position délicate lors d'un contentieux ;
- les traces d'accès au DPI sont conservées sans limitation de temps, depuis l'installation du système.

203. **Les actions des utilisateurs du DPI doivent faire l'objet de mesures de traçabilité**. On pourra pour cela se référer à la recommandation de la CNIL relative à la journalisation[62]. En particulier, les connexions au DPI (identifiants, date et heure), les recherches de dossiers, les consultations d'informations et les opérations réalisées sur celles-ci (ajouts, modifications, suppressions) doivent être tracées, pour l'ensemble des données structurées et des documents rattachés au DPI.

204. Cette journalisation est assurée au niveau applicatif et génère des « **traces fonctionnelles** » qui doivent permettre de documenter les accès et les modifications sur le contenu du dossier médical, avec leur auteur et leur date.

205. Elles doivent être accessibles aux professionnels de santé afin d'informer l'équipe de soins et lui permettre de retracer le parcours d'un patient (professionnels ayant participé aux précédentes prises en charge, actes et éléments de décision associés, etc.), lui permettant ainsi de comprendre, voire de questionner, les orientations thérapeutiques.

206. Les traces fonctionnelles assurent également la transparence des accès et des décisions médicales en cas de contentieux, de violation du secret professionnel ou de violation de données.

207. Par conséquent, **les traces fonctionnelles doivent être stockées au sein du DPI avec les mêmes règles de confidentialité** que le dossier patient auxquelles elles se rapportent. **De même, les traces de consultations et d'actions en lien avec le parcours de soin du patient** (diagnostic, orientation thérapeutique, prescription, etc.) **doivent être conservées avec la même durée** que son dossier (20 ans après la dernière visite dans l'établissement). Afin de disposer d'une valeur probante[63], la CNIL recommande que ces traces soient non modifiables, enregistrées en lecture seule et de manière cloisonnée.

208. En parallèle, des « **traces techniques** » sont générées par les systèmes informatiques sous-jacents (serveurs, pare-feu, actifs réseaux, etc.) afin de permettre la détection et l'analyse des incidents de sécurité et des violations de données. Elles **doivent tracer les flux d'information, avec leur origine et leur destination, leur horodatage précis et leur auteur** (utilisateur ou machine). Elles ne doivent pas contenir de données de santé.

209. Enfin, **les accès en mode « bris de glace » doivent faire l'objet de traces spécifiques** incluant le nom de l'utilisateur et la **justification de son accès**.

210. Afin de résister à un attaquant cherchant à effacer ses traces, **la CNIL recommande que les traces techniques soient stockées en dehors du DPI**, dans une zone protégée, en accès limité et en lecture

[62] À date, délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation. « La CNIL publie une recommandation relative aux mesures de journalisation », CNIL : https://www.cnil.fr/fr/la-cnil-publie-une-recommandation-relative-aux-mesures-de-journalisation

[63] Au sens des articles L. 1111-25 et suivants du CSP

seule, pour une durée d'un an, avec un mécanisme de purge automatique à l'issue de ce délai. Elles doivent être uniquement accessibles aux administrateurs et aux outils de surveillance.

211. En particulier, **les accès des administrateurs aux systèmes internes et aux systèmes externalisés doivent faire l'objet d'une journalisation technique renforcée**. À cet égard, la CNIL recommande la mise en place d'un bastion d'administration avec une authentification multifacteur, permettant d'enregistrer toutes les sessions d'administration et le détail des actions réalisées par chaque administrateur. Les accès en mode dégradé doivent être encadrés par des procédures strictes assurant notamment leur validation hiérarchique, leur traçabilité et leur imputabilité.

212. **Un contrôle des traces fonctionnelles doit être réalisé régulièrement. La CNIL recommande que ce contrôle soit effectué *a minima* mensuellement**, de préférence par une commission interne chargée de surveiller le bon usage du DPI et de traiter les plaintes, et le cas échéant d'effectuer des rappels à l'ordre ou des avertissements. Pour cela, elle peut disposer d'outils d'analyse des comportements utilisateurs, basés sur des règles métiers (par exemple, nombre de professionnels accédant à un même dossier patient, nombre de dossiers consultés chaque jour par un même professionnel, volume de documents consultés, etc.), avec un suivi spécifique des accès en mode « bris de glace ».

213. **Un contrôle régulier des traces techniques doit également être opéré**, par exemple à l'aide de solutions de surveillance automatique remontant des alertes qui seront traitées dans les meilleurs délais par un opérateur habilité. La CNIL recommande de définir des règles d'alertes basées sur des critères techniques qui seront ajustés sur l'activité courante de l'établissement, afin de détecter les activités anormales ou atypiques (par exemple, nombre de connections d'une même adresse IP, localisation géographique, volume de données échangées, etc.).

214. **Une procédure de gestion d'incident doit être définie au préalable, sa mise en œuvre doit être vérifiée régulièrement et elle doit être tenue à jour**. Les incidents et les violations de données doivent faire l'objet d'une consolidation régulière afin de déterminer et de mettre en œuvre des mesures correctives et préventives.

Fiche 14 : les sous-traitants, destinataires et tiers

A. Les sous-traitants

215. La mise en œuvre et le fonctionnement quotidien d'un DPI conduit, dans la majorité des cas, à **l'intervention, ponctuelle ou pérenne, d'un ou plusieurs organismes tiers**.

216. Ces organismes pourront être **qualifiés de sous-traitant** dès lors :

- qu'il s'agit d'une entité juridique distincte du responsable de traitement (personne morale ou physique) ;
- qu'ils traitent des données à caractère personnel pour le compte du responsable de traitement[64].

Cette qualification au titre du RGPD doit être réalisée au cas par cas en tenant compte du contexte et des activités concrètes réalisées par ces organismes.

Les autorités de contrôle ne sont pas liées par la qualification retenue dans un contrat et peuvent, si elles l'estiment nécessaire, requalifier le rôle des parties au regard des opérations effectivement réalisées.

217. Peuvent par exemple être qualifiés de sous-traitant (liste non limitative) :

- les éditeurs des logiciels utilisés pour la mise en œuvre du DPI, notamment si ceux-ci participent à son fonctionnement et sa maintenance ;
- les sociétés proposant une offre d'hébergement, physique ou numérique, des données contenues dans le DPI ;
- les prestataires contribuant à la maintenance et/ou à la sécurité du DPI ;
- les prestataires proposant des services de type conciergerie, notamment pour la mise à disposition de services au sein de la chambre des patients ;
- les prestataires proposant des services de restauration, notamment pour la préparation de repas adaptés à la situation médicale de la personne ;
- les prestataires proposant des services de prise de rendez-vous ;
- les entreprises produisant ou commercialisant un produit de santé utilisé ou ayant vocation à être utilisé lors de la prise en charge de la personne.

218. L'intervention d'un sous-traitant **ne suppose pas nécessairement un accès au DPI ou à l'ensemble des données qu'il contient**. Dans certains cas, il se peut que le personnel habilité du sous-traitant soit destinataire d'une copie de certaines données à caractère personnel issues du DPI. En tout état de cause, **seules les données strictement nécessaires à l'exercice des missions confiées par le responsable de traitement doivent être accessibles ou transmises** au sous-traitant.

219. Le responsable de traitement devra porter une attention particulière :

- aux modalités de consultation des données contenues dans le DPI (accès au DPI, transmission d'une copie, visualisation) ;
- à l'étendue des données à caractère personnel consultables par le sous-traitant (par exemple un épisode de soins, l'ensemble des prises en charge intervenues pendant une période donnée).

1. Cas particulier des sous-traitants avec accès aux données

220. L'accès aux données contenues dans le DPI doit être limité aux seules personnes habilitées en raison de leurs fonctions, et en distinguant les différentes opérations qu'elles peuvent effectuer sur les données. **La CNIL recommande que ces habilitations et les opérations pouvant être effectuées par le sous-**

[64] Pour plus de précisions sur la notion de sous-traitant, voir les lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD (PDF, 1,5 Mo), CEPD : https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_fr.pdf

traitant et les personnes agissant sous sa responsabilité soient déterminées dans le cadre d'une matrice d'habilitation. Cette matrice pourrait être annexée au contrat conclu en application de l'article 28 (voir la Fiche 15 – Partie A).

2. Cas particulier des sous-traitants disposant d'une copie des données

221. Les copies de données à caractère personnel issues du DPI et réalisées pour l'exécution d'un contrat de sous-traitance doivent faire l'objet d'une attention particulière. Aussi le contrat de sous-traitance conclu devra encadrer :

- le périmètre précis des données et des documents concernés, ainsi que leur profondeur historique, au regard des missions confiées au sous-traitant ;
- les modalités de conservation de ces copies ;
- leur durée de conservation, étant précisé que ces copies ne pourront être conservées que pour la durée nécessaire à l'exercice de la mission confiée ;
- les modalités de destruction et /ou de restitution des données à caractère personnel transmises.

222. Il est rappelé que le responsable de traitement est tenu de s'assurer que le traitement et la conservation des copies du DPI par son sous-traitant sont conformes à la règlementation applicable.

3. Cas particulier de la société d'hébergement des données de santé

223. Dès lors que le responsable de traitement a recours aux services d'un tiers pour l'hébergement, le stockage ou la conservation des données de santé collectées pendant la prise en charge de la personne, **ce tiers devra être un hébergeur de données de santé certifié** conformément aux dispositions du CSP[65].

224. Ce tiers ainsi que le personnel agissant sous son autorité sont soumis au secret professionnel.

225. Le recours à un hébergeur/infogéreur pour les données d'un établissement de santé doit respecter les dispositions du CSP et, s'agissant plus particulièrement d'un hébergement sur support électronique, le recours à un hébergeur certifié HDS[66]. **La CNIL souligne trois nouvelles exigences** apportées par la version 2024 du référentiel de certification[67] :

- **hébergement exclusivement sur le territoire européen** ;
- **encadrement des accès à distance** depuis l'extérieur du territoire européen ;
- **transparence sur les risques associés aux législations extra-européennes** auxquelles seraient soumis l'hébergeur.

La CNIL recommande de tenir compte de ces éléments à l'occasion du renouvellement du certificat d'un hébergeur du DPI[68], ainsi qu'au moment de la reconduction de son contrat ou du choix d'un nouvel hébergeur.

B. Les tiers : destinataires et tiers autorisés

226. La notion de tiers utilisée dans cette partie renvoie à la définition prévue par l'article 4.10 du RGPD. Cette notion peut donc avoir un périmètre plus large que la notion de personne tierce à l'équipe de soins ou à l'établissement de santé, responsable de traitement.

227. La transmission de données à caractère personnel contenues dans le DPI à des tiers peut s'avérer nécessaire :

- en application de la règlementation en vigueur ;

[65] Article L.1111-8 du code de la santé publique.

[66] « Certification des hébergeurs de données de santé », ANS : https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante et « Arrêté du 26 avril 2024 modifiant l'arrêté du 11 juin 2018 », Légifrance : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049537692

[67] Référentiels de la certification HDS. « Les référentiels de la procédure de certification », ANS : https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification

[68] La nouvelle version du référentiel HDS s'applique pour une demande initiale ou pour le renouvellement de la certification d'un hébergeur, qui a lieu tous les trois ans, donc au plus tard en octobre 2027.

- pour garantir la coordination des soins avec des professionnels intervenant dans la prise en charge de la personne concernée.

228. Dans tous les cas, les principes relatifs au traitement des données à caractère personnel consacrés par le RGPD restent applicables[69].

1. Les tiers susceptibles d'intervenir dans la prise en charge des patients

a. L'équipe de soins étendue hors de l'établissement de santé

229. La notion d'équipe de soins est liée au parcours de santé de la personne concernée. Elle peut ainsi inclure des professionnels de santé exerçant en dehors de l'établissement de santé responsable du DPI (professionnel exerçant dans un autre établissement de santé ou en ville, médecin traitant).

230. Les conditions pour qu'un professionnel de santé appartienne à l'équipe de soins s'appliquent telles que mentionnées ci-dessus (Voir la Fiche 12 – Partie A.1).

231. En principe, ces professionnels externes à l'établissement n'ont pas accès aux documents contenus au sein du DPI et sont destinataires d'une copie de données ou de documents composant le DPI.

232. La transmission de données à caractère personnel, incluses ou non dans un document du DPI, peut intervenir soit de manière :

- « automatique ». C'est notamment le cas des lettres de liaison éditées à la fin d'une hospitalisation qui doivent être transmises au professionnel qui a adressé le patient à l'établissement de santé et à son médecin traitant[70] (en dehors de l'équipe de soins se référer aux conditions de la Fiche 12 – Partie A.2) ;
- à la demande du patient. Le patient peut communiquer à l'établissement de santé, les coordonnées des professionnels de santé intervenant dans sa prise en charge et pour lesquels il souhaite que des données à caractère personnel le concernant, soient communiquées[71]. Le patient étant susceptible de changer d'avis ou de ne plus être suivi par le professionnel concerné, il est recommandé de les tenir à jour, notamment en demandant au patient de confirmer sa demande.

a. Professionnels participant à la prise en charge de la personne mais ne relevant pas de l'équipe de soins

233. Certains professionnels, relevant des catégories mentionnées à l'article R. 1110-2, mais ne faisant pas partie de l'équipe de soins, peuvent avoir besoin d'accéder aux données de santé contenues dans le DPI, pour le consulter et y verser des documents utiles à la prévention, la continuité et la coordination des soins. Une information détaillée concernant notamment les catégories de données à caractère personnel ayant vocation à être partagées et les catégories de professionnels fondés à en connaître doit lui être fournie. Son consentement à partager ces données est également requis[72].

2. Les tiers autorisés

234. Certaines autorités publiques ont le pouvoir d'exiger la transmission de données à caractère personnel ou de documents, en vertu de l'intérêt public qui s'attache à l'accomplissement de leurs missions. L'enjeu pour l'établissement de santé recevant une telle demande est de veiller à se conformer aux dispositions légales tout en garantissant la sécurité des données à caractère personnel traitées.

235. Ainsi, à réception d'une demande d'accès ou de transmission, le responsable doit s'interroger sur :

- l'existence d'une base légale fondant la demande de l'autorité et autorisant la communication des données ;
- la qualité de l'organisme à l'origine de la demande et le périmètre des données à caractère personnel ciblées ;

[69] Article 5 du règlement général sur la protection des données.
[70] Article L.1112-1 du code de la santé publique.
[71] Article L. 1111-2 du code de la santé publique.
[72] Article D. 1110-3-1 du code de la santé publique.

- les moyens de sécuriser la communication des seules données nécessaires ou les modalités d'accès par le tiers autorisé[73].

236. La CNIL a publié un guide pratique et un recueil des procédures les plus courantes afin d'aider les professionnels visés par ce type de demande[74].

237. Concernant le DPI, les tiers autorisés peuvent notamment être :

- les commissaires aux comptes dans le cadre de l'exercice de leur mission[75]. Les conditions d'accès sont précisées dans le CSP[76] ;
- les forces de l'ordre et la justice (police, gendarmerie, juge, procureur de la République). Il existe différentes procédures susceptibles de justifier une transmission de données à caractère personnel : l'enquête préliminaire[77], l'enquête de flagrance[78], l'enquête d'instruction[79] ;
- la commission de conciliation et d'indemnisation[80] (CCI) qui, avant d'émettre son avis, peut diligenter une expertise et obtenir communication de tout document, y compris d'ordre médical[81] ;
- les médecins de l'inspection générale des affaires sociales, les médecins inspecteurs de santé publique, les médecins de l'agence régionale de santé, les médecins conseils des organismes d'assurance maladie[82], lorsqu'elles sont nécessaires à l'exercice de leurs missions ;
- les médecins-experts dans le cadre de la certification menées par la Haute autorité de santé (HAS) [83].

238. L'ensemble de ces tiers autorisés a accès aux données de santé à caractère personnel strictement nécessaires à l'exercice de leur mission, dans le respect du secret professionnel.

3. Les attachés de recherche clinique et les techniciens d'études cliniques.

239. Concernant les ARC et les TEC externes à l'établissement, ils peuvent, dans le cadre des contrôles menés pour s'assurer de la qualité de la recherche, accéder au DPI sur place. Outre les obligations prévues à l'article L. 1121-3 du CSP, il est recommandé de respecter les modalités d'accès décrites dans les méthodologies de référence publiées par la CNIL[84].

C. Les mesures de sécurité associées

240. On veillera à mettre en œuvre les mesures de sécurité applicables décrites dans la présente recommandation, en particulier celles de la Fiche 9 pour les échanges de données, de la Fiche 13 pour les accédants au DPI (authentification, habilitations, traçabilité) et de la Fiche 15 pour les relations avec les sous-traitants et les tiers.

[73] Articles 5-1-f et 32 du règlement général sur la protection des données.
[74] Site internet de la CNIL, « Tiers autorisés : la CNIL publie un guide pratique et un recueil de procédures ».
[75] Article L. 823-9 du code du commerce et article L. 6113-7 du code de la santé publique.
[76] Articles R. 61113-5 et suivants du code de la santé publique.
[77] Article 77-1-1 du code de procédure pénale : la remise directe ou spontanée de document sur réquisition est obligatoire pour les informations/documents administratifs mais facultative pour les documents médicaux.
[78] Article 60-1 du code de procédure pénale : la remise directe ou spontanée de document sur réquisition est obligatoire pour les documents administratifs mais facultative pour les documents médicaux.
[79] Articles 96 et 97 du code de procédure pénale : la saisie sur commission rogatoire du dossier médical est possible et ne peut être refusée.
[80] Article L. 1142-5 du code de la santé publique.
[81] Article L. 1142-9 du code de la santé publique.
[82] Article L. 1112-1 du code de la santé publique.
[83] Article L. 1414-4 du code de la santé publique.
[84] Par exemple : délibération n° 2018-153 du 3 mai 2018 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé avec recueil du consentement de la personne concernée (MR-001) et abrogeant la délibération n° 2016-262 du 21 juillet 2016.

Fiche 15 : la maîtrise des relations avec les sous-traitants et les tiers

241. Comme pour tout traitement de données à caractère personnel, les interactions avec des destinataires (sous-traitants, éditeurs de logiciel, tiers) sont soumises à des exigences règlementaires. En outre, ces relations constituent des sources potentielles de vulnérabilités. En conséquence, un soin particulier doit être apporté à la gestion des relations avec les différentes parties intervenant dans le cadre du DPI.

A. Les relations avec les sous-traitants

Problèmes constatés :

- Le contrat de sous-traitance conclu n'est pas conforme à l'article 28 du RGPD. Il ne précise pas l'objet, la durée et la finalité du traitement, les catégories de données à caractère personne traitées et les catégories de personnes concernées.
- Les caractéristiques de la prestation réalisée par le sous-traitant sont précisées dans le cadre de correspondances entre l'établissement de santé et le prestataire. Ces éléments ne sont pas inclus dans un contrat ou un acte juridique.
- Absence d'installation de mise à jour de sécurité des logiciels utilisés pour le DPI.

242. L'établissement de santé est tenu de **faire appel à des sous-traitants qui présentent des garanties techniques et organisationnelles suffisantes pour la protection des données traitées**, notamment leur confidentialité et leur intégrité.

243. À ce titre, l'établissement de santé **évalue les garanties fournies par chaque sous-traitant avant leur sélection**. Il est recommandé que l'établissement choisisse ses sous-traitants au regard de leur capacité à respecter un cahier des charges établi à l'avance[85]. Outre les connaissances spécialisées du sous-traitant, sa fiabilité et ses ressources, une attention particulière devra être portée sur le niveau de service qu'il est susceptible de garantir concernant la sécurité des systèmes d'information.

244. Afin de garantir une parfaite maîtrise sur le long terme de la sécurité du DPI et des données à caractère personnel traitées pendant toute la durée d'exécution de la prestation, **des audits réguliers doivent être menés**. À cet égard, il est recommandé de faire appel à des prestataires qualifiés par l'ANSSI[86].

245. Cette démarche peut, à titre de bonne pratique, s'appuyer sur des normes reconnues de cybersécurité (ISO 27001) et de protection de la vie privée (ISO 27701), qui prévoient des certificats de conformité établis par des organismes d'audit indépendants[87]. Dans ce cas, l'établissement est encouragé à vérifier que le périmètre de certification d'un sous-traitant correspond au service visé et contrôler le bon renouvellement de cette certification en fin de validité (en général, tous les trois ans).

246. L'établissement de santé est tenu de **conclure, avec chacun de ses sous-traitants, un acte juridique écrit qui engage les parties**, le plus souvent un contrat. Ce document devra couvrir l'ensemble des points mentionnés à l'article 28 du RGPD. Ce contrat pourra être fondé, en tout ou partie, sur les clauses contractuelles types établies par la Commission européenne[88], sous réserve que les dispositions nationales applicables soient prises en compte (par exemple les spécificités applicables aux prestations d'hébergement des données de santé).

[85] Ce cahier des charges pourra prendre en compte les mesures de sécurité développées *Infra*.
[86] Prestataires d'audit de la sécurité des systèmes d'information (PASSI). « Référentiels d'exigences pour la qualification », ANSSI : https://cyber.gouv.fr/referentiels-dexigences-pour-la-qualification
[87] La certification des hébergeurs de données de santé (HDS) est basée sur l'ISO 27001
[88] « Décision d'exécution - 2021/915 – EN », EUR-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32021D0915

247. Par ailleurs, la CNIL recommande que le document contractuel :

- détaille la **répartition des obligations notamment en matière de sécurité**. En particulier, les exigences de sécurité pour les sous-traitants liés au DPI doivent être formalisées et détaillées, par exemple sous la forme de SLA (*service-level agreement*) et de PAS (Plan d'assurance sécurité), à la hauteur des exigences de sécurité identifiées pour le DPI ;
- prévoit des **conditions de fin de contrat et de réversibilité soutenables** pour l'établissement de santé, notamment par le maintien de la prestation sous sa forme initiale pendant un délai suffisant à l'organisation d'une migration vers un autre prestataire. Un délai de deux ans pour les sous-traitants les plus impliqués dans la mise en œuvre du DPI semble adapté aux enjeux ;
- prévoit une **information de l'établissement de santé en cas de changement de contexte** susceptible d'impacter les conditions d'exécution de la prestation conclue ;
- impose d'obtenir **l'accord préalable et spécifique de l'établissement** de santé de tout changement concernant l'ajout ou la modification d'un sous-traitant ultérieur traitant les données du DPI ;
- **liste précisément et limitativement les finalités pour lesquelles les données traitées par le sous-traitant peuvent être réutilisées** par celui-ci. Dans cette hypothèse, il appartient à l'établissement de santé de s'assurer de la compatibilité des finalités poursuivies ultérieurement et d'informer les personnes de ces réutilisations[89].

248. Les personnels des sous-traitants doivent être spécifiquement habilités à accéder au DPI, sur un périmètre précisément défini. En fonction des tâches qui leurs sont confiées, il peut être nécessaire d'appuyer cette habilitation sur **une clause de confidentialité spécifique**.

249. Si la prestation fournie par le sous-traitant implique des transferts de données en dehors de l'Union européenne, dont des accès distants aux données depuis l'extérieur du territoire européen, ceux-ci devront être conformes au chapitre V du RGPD.

B. Les relations avec les éditeurs de solutions (hors sous-traitances)

250. L'établissement de santé est tenu **d'utiliser des solutions permettant de garantir la protection des données traitées**, notamment leur confidentialité et leur intégrité.

251. À ce titre, il est recommandé que l'établissement sélectionne ses solutions au regard de leur capacité à respecter un cahier des charges établi à l'avance, avec une attention particulière pour les exigences relatives à la sécurité des systèmes d'information, et en particulier pour la capacité de mettre en œuvre les mesures portées par la présente recommandation.

252. Les services numériques en santé utilisés par les établissements de santé doivent désormais être conformes à des référentiels produits par l'Agence du numérique en santé (ANS) et rendus opposables par voie d'arrêté du ministre chargé de la santé[90]. Pour certains de ces référentiels, l'arrêté peut prévoir la délivrance d'un certificat de conformité par l'ANS[91].

253. Le DPI constituant un service numérique de santé, il appartient à l'établissement de santé de s'assurer que le service utilisé dispose des certificats de conformité nécessaires en application de la règlementation. A cet égard, une liste des services numériques certifiés est mis à disposition du public par l'ANS.

---

[89] Voir fiche n°10 et l'article à ce sujet sur le site de la CNIL. « Sous-traitants : la réutilisation de données confiées par un responsable de traitement », CNIL : https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement

[90] Article L. 1470-5 du CSP : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043497489. C'est le cas par exemple :

- des référentiels relatif à l'identification des usagers du système de santé, Légifrance : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045457991
- du référentiel DMP, Légifrance : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048368244 ; et
- du référentiel ProSantéConnect, Légifrance : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045551195

[91] Article L. 1470-6 du CSP, Légifrance : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000046822530 ; c'est notamment le cas pour les systèmes d'information de téléconsultation : arrêté du 9 février 2024, Légifrance : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049122111

254. De plus, certains financements publics pour des solutions logicielles en santé sont conditionnés au respect d'un cahier des charges de sécurité[92].

255. Enfin, pour assurer la maîtrise sur le long terme de la sécurité et de la conformité du DPI, la CNIL recommande de **sélectionner des offres de solutions incluant un contrat de maintenance corrective et évolutive, avec des mises à jour régulières**.

C. Les relations avec les tiers

256. Les relations avec les tiers devraient également être formalisées. A cet égard, **la CNIL recommande que les transmissions de données fassent l'objet d'un contrat** définissant précisément les données transmises et la finalité poursuivie ultérieurement, ainsi que les mesures de sécurité de ces transmissions.

257. Préalablement à la transmission de données, **l'établissement de santé doit déterminer si la finalité du traitement ultérieur est compatible** avec la finalité pour laquelle les données ont été initialement collectées[93].

258. Les transmissions de données vers des partenaires **devraient être tracées et reposer sur des canaux sécurisés** ; les données transmises doivent être chiffrées avec des mécanismes conformes au référentiel général de sécurité[94].

259. Si la transmission de données du DPI à des tiers implique des transferts de données en dehors de l'Union européenne, ceux-ci devront être conformes au chapitre V du RGPD.

[92] Par exemple, le « Ségur du Numérique », « Les dispositifs de la vague 2 du Ségur du numérique en santé », ANS : https://industriels.esante.gouv.fr/segur-numerique-sante/vague-2 et les financements associés au programme « CaRE - Cybersécurité accélération et Résilience des Établissements », ANS : https://esante.gouv.fr/espace-presse/presentation-du-programme-care

[93] « Sous-traitants : la réutilisation de données confiées à un responsable de traitement », CNIL : https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement

[94] « RGS », ANSSI : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs

Fiche 16 : la sécurisation des opérations de maintenance

Problèmes constatés :

- Une extraction de données, réalisée en vue d'effectuer la migration d'un système de gestion de bases de données, est stockée puis oubliée sur un répertoire temporaire insuffisamment sécurisé.
- La copie de test d'une base de données, contenant des données réelles, est rendue accessible pour les développeurs via Internet, avec un simple mot de passe (ou aucun).
- Des prestataires de maintenance disposent d'un accès permanent au système d'information, à distance et avec des droits d'administration.
- Le DPI est rendu indisponible par un problème non anticipé lié à la mise à jour de sa base de données.

260. **Les interventions de support et de maintenance à distance présentent des risques élevés**, en ce qu'elles font intervenir des personnels qui ne sont pas nécessairement connus à l'avance, le plus souvent à distance, et qu'elles peuvent exposer des volumes massifs de données à caractère personnel sensibles.

261. Ces interventions doivent être encadrées par des contrats et des procédures, définis le plus possible en amont du besoin ou de l'incident. Elles doivent toutes faire l'objet d'un compte rendu détaillé, validé et conservé par l'établissement.

262. La CNIL recommande que ces interventions soient réalisées à travers des accès temporaires, ouverts ponctuellement et refermés dès la bonne fin de l'intervention. Ces accès seront créés avec une période de validité réduite pour garantir leur désactivation automatique en cas d'oubli. En outre, la CNIL recommande l'utilisation d'un bastion d'administration en authentification multifacteur, permettant d'assurer la traçabilité complète des sessions d'intervention pour chaque utilisateur.

263. Les opérations de migrations de données, ainsi que les opérations de tests techniques et fonctionnels qui les accompagnent, présentent des risques particuliers. En effet, outre les risques sur l'intégrité ou la disponibilité des données liés à la migration elle-même, la montée de version d'un logiciel, le remplacement d'un système de base de données ou d'une baie de stockage, *etc.* nécessitent souvent d'exporter les données, d'en créer des copies de sauvegarde ou de test et de les stocker sur des espaces de travail temporaires.

264. **Ces espaces de travail doivent faire l'objet de mesures renforcées de contrôle d'accès et de traçabilité, en tenant compte notamment des risques liés à l'intervention de prestataires internes et externes**. Ces espaces doivent être protégés et sauvegardés dans les mêmes conditions de sécurité que le DPI (voir notamment les Fiches 6, 7, 9 et 13), et leur purge doit être assurée à la bonne fin des opérations et au plus tard dans un délai défini, qui ne pourra être prolongé que sur décision hiérarchique, explicite et tracée.

265. Enfin, dans l'objectif général d'assurer le maintien en condition opérationnelle du DPI et l'intégrité de ses données, il est de bonne pratique que toute mise en production soit accompagnée d'une procédure de retour arrière en cas de problème, laquelle devra également avoir été testée au préalable.

Glossaire

- **donnée à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (article 4-1) du RGPD) ;
  - **données concernant la santé** : les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne (article 4-15) du RGPD) ;
  - **données génétiques** : données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question (article 4-13) du RGPD) ;
  - **données concernant des personnes vulnérables** : données concernant des personnes pour lesquelles un déséquilibre des pouvoirs existe entre le responsable de traitement et les personnes concernées. Cela concerne par exemple les patients, les personnes âgées, les mineurs, les personnes souffrant de maladie mentale, et plus généralement toute situation dans laquelle les personnes peuvent se trouver dans l'incapacité de consentir, ou de s'opposer, aisément au traitement de leurs données ou d'exercer leurs droits[95]. La notion de personnes vulnérables au sens du RGPD ne couvre donc pas exclusivement les mineurs ou les majeurs protégés ;
- **traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction (article 4-2) du RGPD) ;
  - **responsable de traitement** : l'établissement de santé de droit public ou de droit privé qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement nécessaire à celle-ci (article 4-7) du RGPD) ;
  - **sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement (article 4-8) du RGPD). Il s'agit par exemple des éditeurs des services ou outils numériques, des entreprises exploitant ou fabricant un dispositif médical ou de prestataires d'hébergement des données de santé ;
  - **destinataire** : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers (article 4-9) du RGPD). Il s'agit par exemple des professionnels de santé n'exerçant pas au sein de l'établissement qui appartiennent à l'équipe de soin de la personne ;
  - **accédant** : le personnel habilité du responsable de traitement ou d'un sous-traitant qui accède au DPI ou aux systèmes sur lesquels il repose ;
  - **tiers** : une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel (article 4-10) du RGPD) ;

[95] Considérant (75) du RGPD et « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 ».

- service numérique en santé : les systèmes d'information ou les services ou outils numériques mis en œuvre par des personnes physiques ou morales de droit public ou de droit privé, y compris les organismes d'assurance maladie, proposés par voie électronique, qui concourent à des activités de prévention, de diagnostic, de soin ou de suivi médical ou médico-social, ou à des interventions nécessaires à la coordination de plusieurs de ces activités[96] . Il s'agit, par exemple, des systèmes utilisés pour la mise en œuvre des dossiers patients informatisés ;
    - **dossier patient** : traitement des données à caractère personnelles collectées à l'occasion d'une prise en charge sanitaire, médico-sociale ou des activités nécessaires à la coordination de ces prises en charge. Le terme dossier patient informatisé (DPI) renvoie aux traitements mis en œuvre sur support numérique ;
    - **secret professionnel** : secret professionnel mentionné à l'article L. 1110-4 du code de la santé publique (CSP) s'imposant à l'ensemble des professionnels, des établissements et des services concourant à la prévention ou aux soins ;
    - **identification** : processus consistant à utiliser des données d'identification personnelle représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale (article 3 du règlement (UE) n°910/2014) ;
        - **identitovigilance** : l'organisation et les moyens mis en œuvre par un établissement ou un professionnel de santé pour fiabiliser et sécuriser l'identification de l'usager à toutes les étapes de sa prise en charge[97] ;
        - **identifiant national de santé (INS)** : numéro d'inscription au répertoire national d'identification (NIR) des personnes physiques utilisé pour la prise en charge sanitaire et médico-sociales des personnes lorsqu'il a été vérifié par l'appel au téléservice dédié de l'Assurance maladie ;
    - **authentification** : un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique (article 3 du règlement (UE) n°910/2014) ;
- **dispositif médical** : tout instrument, appareil, équipement, logiciel, implant réactif destiné, par le fabricant, à être utilisé à des fins médicales telles que précisées à l'article 2 du règlement (UE) 2017/745[98] ;
- **portail de transparence** : page web dédiée à l'information des personnes concernant les traitements ultérieurs réutilisant les données à caractère personnel collectées dans le cadre de la prise en charge des personnes. Cette page web est diffusée sur le site web du responsable du traitement initial, l'établissement de santé à l'origine de la collecte des données, et fournit aux personnes l'ensemble des informations prévues à l'article 14 du RGPD s'agissant des traitements ultérieurs mis en œuvre.

[96] Article L. 1470-1 du code de la santé publique.

[97] « Référentiel national d'identitovigilance (RNIV) : Identitovigilance en établissements de santé » du Ministère de la santé et de la prévention, ANS : https://esante.gouv.fr/espace_documentation/identite-nationale-de-sante/2-mise-en-oeuvre-de-lidentitovigilance-dans-les-etablissements-de-sante

[98] « Règlement (UE) 2017/745 du Parlement européen et du Conseil », EUR-Lex : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32017R0745