AGENCE
DU NUMÉRIQUE
EN SANTÉ

Déclaration de conformité aux dispositions législatives et réglementaires relatives à la protection des données à caractère personnel des exploitants de dispositifs médicaux numériques

Statut :	*Classification :*	Version : *V1.2.0*
Validé	*Publique*	*11/05/2023*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Déclaration de conformité aux dispositions législatives et réglementaires relatives à la protection des données à caractère personnel des exploitants de dispositifs médicaux numériques

Ce document s'adresse aux exploitants de dispositifs médicaux numériques (DMN)[1] souhaitant s'inscrire dans un dispositif de prise en charge ou de remboursement par l'Assurance Maladie.

Il a pour objet de rappeler aux exploitants de DMN que leurs dispositifs doivent être conformes à l'ensemble des dispositions législatives et réglementaires relatives à la protection de données personnelles, notamment à celles de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ainsi que, le cas échéant, aux règles relatives à l'hébergement des données de santé prévu par l'article L. 1111-8 du code de la santé publique.

Le respect de ces dispositions constitue un prérequis au dépôt d'une demande de certification de conformité au référentiel d'interopérabilité et de sécurité des dispositifs médicaux numériques.

En cas de non-respect de ces dispositions, tout exploitant de DMN s'expose à des sanctions en cas de contrôle par la Commission nationale de l'informatique et des libertés (CNIL), conformément à l'Article 58 du RGPD.

Nom de l'exploitant de DMN :

Nom du DMN concerné par la demande de certification de conformité et son numéro de version :

☐ En cochant cette case, **je déclare avoir pris les mesures permettant la sécurité des traitements,** conformément à l'article 32 du RGPD.*

- de l'Article 32 du RGPD – Sécurité du traitement : :
    - 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

      a) la pseudonymisation et le chiffrement des données à caractère personnel ;

      b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

      c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

      d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

    - 2. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de

[1] On appelle Dispositifs Médicaux Numériques "Tout logiciel répondant à la définition du dispositif médical énoncée à l'article 2 du règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE."

données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

- 3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 peut servir d'élément pour démontrer le respect des exigences prévues au paragraphe 1 du présent article.

- 4. Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.

☐ En cochant cette case, **je déclare,** dans la mesure où le traitement porte sur les données sensibles et/ou est réalisé à grande échelle, **avoir réalisé une analyse d'impact relative à la protection des données,** conformément à l'article 35 du RGPD.*

- De l'Article 35 du RGPD - Analyse d'impact relative à la protection des données, notamment :

  - Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

☐ En cochant cette case, **je déclare veiller à ce que mes sous-traitants présentent des garanties suffisantes en matière de protection des données et avoir conclu un contrat de sous-traitance avec ces derniers,** conformément à l'article 28 du RGPD.*

- de l'Article 28 du RGPD – Sous-traitant, notamment :

Le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement. Ce contrat ou cet autre acte juridique prévoit, notamment, que le sous-traitant :

a) ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel le sous-traitant est soumis; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public;

b) veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;

c) prend toutes les mesures requises en vertu de l'article 32 ;

d) respecte les conditions visées aux paragraphes 2 et 4 pour recruter un autre sous-traitant ;

e) tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits prévus au chapitre III ;

f) aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;

g) selon le choix du responsable du traitement, supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel ; et

h) met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent article et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits (…).

[*] *L'engagement à respecter les articles 28, 32 et 35 ne s'appliquent à l'ENS que dans le cadre de la réglementation applicable, à savoir, quand elle est responsable de traitement. Dans le cas contraire l'ENS n'est tenue qu'à une obligation de conseil et il lui appartient d'intervenir en tant que de besoin pour assister le responsable de traitement dans la rédaction de l'Etude d'Impact sur la Vie Privée (Privacy Impact Assessment »).*

La présente déclaration est à joindre au dossier de demande de certification de conformité au référentiel d'interopérabilité et de sécurité

Fait le :

Prénom, Nom et signature du représentant de l'exploitant de DMN :