Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

Décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel

NOR : *SSAZ1733293D*

Publics concernés : *patients ; personnes physiques ou morales responsables de traitements de données de santé à caractère personnel ; prestataires qui concourent à la fourniture d'un service d'hébergement de données de santé à caractère personnel ; organismes de certification.*

Objet : *règles relatives à l'hébergement de données de santé à caractère personnel.*

Entrée en vigueur : *le décret entre en vigueur le lendemain de sa publication, sous réserve des dispositions prévues à l'article 3.*

Notice : *le décret précise le champ des activités d'hébergement de données de santé à caractère personnel qui sont soumises à un agrément délivré par le ministre chargé de la santé ou à une certification. Il détermine les conditions d'application de l'obligation, pour toute personne physique ou morale à l'origine de la production ou du recueil de ces données de santé, de recourir à un hébergeur certifié ou agréé lorsqu'il externalise la conservation des données dont il est responsable.*

Le décret définit le périmètre des activités d'hébergement de données de santé relevant de la certification, fixe les conditions d'obtention du certificat de conformité et les clauses minimales que doit comporter le contrat d'hébergement de données de santé.

Enfin, il précise les conditions dans lesquelles sont régis les demandes d'agrément déposées avant le 31 mars 2018 ainsi que les agréments jusqu'à leur terme.

Références : *le décret est pris pour l'application de l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel. Les dispositions du code de la santé publique modifiées par le présent décret peuvent être consultées, dans leur rédaction résultant de cette modification, sur le site Légifrance (www.legifrance.gouv.fr).*

Le Premier ministre,

Sur le rapport de la ministre des solidarités et de la santé,

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

Vu la directive 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la santé publique, notamment son article L. 1111-8 ;

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

Vu l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, notamment son article 3 ;

Vu l'avis du Conseil national de l'ordre des sages-femmes en date du 11 septembre 2017 ;

Vu l'avis du Conseil national de l'ordre des pédicures-podologues en date du 15 septembre 2017 ;

Vu l'avis du Conseil national de l'ordre des chirurgiens-dentistes en date du 18 septembre 2017 ;

Vu l'avis du Conseil national de l'ordre des médecins en date du 21 septembre 2017 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 12 octobre 2017 ;

Vu l'avis du Conseil national de l'ordre des pharmaciens en date du 6 novembre 2017 ;

Vu la saisine du Conseil national de l'ordre des infirmiers en date du 24 août 2017 ;

Vu la saisine du Conseil national de l'ordre des masseurs-kinésithérapeutes en date du 24 août 2017 ;

Vu la notification n° 2017/343/F adressée le 20 juillet 2017 à la Commission européenne ;

Le Conseil d'Etat (section sociale) entendu,

Décrète :

Art. 1er. – Le code de la santé publique est ainsi modifié :

1° Au premier alinéa de l'article R. 1111-1, les mots : « professionnel de santé, un établissement de santé ou un hébergeur agréé en application de l'article L. 1111-8 » sont remplacés par les mots : « professionnel de santé ou un établissement de santé » et au deuxième alinéa, les mots : « ou à l'hébergeur » sont supprimés ;

2° Au premier alinéa de l'article R. 1111-2, les mots : « professionnel de santé, de l'établissement de santé ou de l'hébergeur » sont remplacés par les mots : « professionnel de santé ou de l'établissement de santé » et au dernier alinéa, les mots : « professionnel de santé, l'établissement de santé ou l'hébergeur » sont remplacés par les mots : « professionnel de santé ou l'établissement de santé » ;

3° Au premier alinéa de l'article R. 1111-3, les mots : « professionnel de santé, l'établissement ou l'hébergeur » sont remplacés par les mots : « professionnel de santé ou l'établissement » et au second alinéa, les mots : « professionnel de santé, l'établissement ou, le cas échéant, l'hébergeur » sont remplacés par les mots : « professionnel de santé ou l'établissement » ;

4° L'article R. 1111-8 est abrogé ;

5° Au dernier alinéa de l'article R. 1111-10, les mots : « de rejet » sont remplacés par les mots : « d'acceptation » ;

6° Les 2° et 3° de l'article R. 1111-13 sont remplacés par les dispositions suivantes :

« 2° Lorsque le contrat est souscrit par la personne concernée par les données hébergées, la description des modalités selon lesquelles les professionnels visés à l'article L. 1110-4 et, le cas échéant, la personne concernée, accèdent à ces données dans le respect des dispositions des articles L. 1110-4 et L. 1110-4-1 ;

« 3° Lorsque le contrat est souscrit par la personne physique ou morale à l'origine de la production ou du recueil des données de santé mentionnée au premier alinéa de l'article L. 1111-8, la description des modalités d'information de la personne concernée et d'enregistrement de l'absence d'opposition pour motif légitime de cette dernière à l'hébergement de ses données de santé, ainsi que des modalités selon lesquelles les professionnels visés à l'article L. 1110-4 et le cas échéant la personne concernée, accèdent à ces données dans le respect des dispositions des articles L. 1110-4 et L. 1110-4-1 ; »

7° A l'article R. 1111-14 :

a) Au *a* du 1°, les mots : « du consentement » sont remplacés par les mots : « de l'information et de l'absence d'opposition pour motif légitime » ;

b) Au *b* du 1°, les mots : « n'aient lieu qu'avec l'accord des personnes concernées et par les personnes désignées par elles » sont remplacés par les mots : « soient réalisées dans le respect des dispositions de l'article L. 1110-4 » ;

c) Au *a* du 2°, les mots : « établissements ou des professionnels de santé à l'origine du dépôt » sont remplacés par les mots : « personnes physiques ou morales à l'origine de la production ou du recueil des données de santé » ;

d) Au *e* du 2°, les mots : « avoir été agréés par le groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale » sont remplacés par les mots : « être conformes aux référentiels de sécurité mentionnés à l'article L. 1110-4-1. » ;

8° Au deuxième alinéa de l'article R. 1111-20-4, les mots : « par l'hébergeur mentionné à l'article R. 1111-20-10 » sont supprimés et au dernier alinéa, les mots : « par l'hébergeur » sont supprimés ;

9° A l'article R. 1111-20-10, les mots : « agréé en application de l'article L. 1111-8 » sont remplacés par les mots : « dans le respect des dispositions de l'article L. 1111-8 » ;

10° Au premier alinéa de l'article R. 1111-20-11, les mots : « par l'hébergeur » sont remplacés par les mots : « dans le dossier pharmaceutique », au deuxième alinéa, les mots : « par l'hébergeur » sont supprimés et le dernier alinéa est remplacé par les dispositions suivantes : « Le refus de création d'un dossier pharmaceutique est conservé dans l'application "dossier pharmaceutique" » durant trente-six mois. » ;

11° Au I, au 1° du II et au 2° du II de l'article R. 1111-20-12, les mots : « conservés par l'hébergeur » sont remplacés par les mots : « conservés dans le dossier pharmaceutique » et les mots : « l'hébergeur détruit ces données » sont remplacés par les mots : « ces données sont détruites. » ;

12° Le 3° de l'article R. 1111-35 est remplacé par les dispositions suivantes :

« 3° Par l'intermédiaire de la Caisse nationale de l'assurance maladie. » ;

13° A l'article R. 1112-7, les mots : « agréé en application des dispositions à l'article L. 1111-8. » sont remplacés par les mots : « dans le respect des dispositions de l'article L. 1111-8. » ;

14° A l'article R. 6316-10, les mots : « dispositions prévues au quatrième alinéa de l'article L. 1111-8 du code de la santé publique relatif aux modalités d'hébergement des données de santé à caractère personnel. » sont remplacés par les mots : « référentiels d'interopérabilité et de sécurité mentionnés à l'article L. 1110-4-1. » et le second alinéa est supprimé.

Art. 2. – I. – Après la sous-section 1 *bis* de la section 1 du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique, il est inséré une sous-section 1 *ter* ainsi rédigée :

« Sous-section 1 ter

« Dispositions générales relatives à l'hébergement de données de santé à caractère personnel

« *Art. R. 1111-8-8.* – I. – L'activité d'hébergement de données de santé à caractère personnel mentionnée au I de l'article L. 1111-8 consiste à héberger les données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social :

« 1° Pour le compte de personnes physiques ou morales, responsables de traitement au sens de la loi n° 78-17 du 6 janvier 1978, à l'origine de la production ou du recueil de ces données ;

« 2° Pour le compte du patient lui-même.

« Toutefois, ne constitue pas une activité d'hébergement au sens de l'article L. 1111-8, le fait de se voir confier des données pour une courte période par les personnes physiques ou morales, à l'origine de la production ou du recueil de ces données, pour effectuer un traitement de saisie, de mise en forme, de matérialisation ou de dématérialisation de ces données.

« II. – Les responsables de traitement mentionnés au 1° du I, qui confient l'hébergement de données de santé à caractère personnel à un tiers, s'assurent que celui-ci est titulaire du certificat de conformité mentionné au II de l'article L. 1111-8. »

II. – La sous-section 2 de la section 1 du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique est remplacée par les dispositions suivantes :

« Sous-section 2

« Hébergement des données de santé à caractère personnel sur support numérique soumis à certification

« *Art. R. 1111-9.* – Est considérée comme une activité d'hébergement de données de santé à caractère personnel sur support numérique au sens du II de l'article L. 1111-8, le fait d'assurer pour le compte du responsable de traitement mentionné au 1° du I de l'article R. 1111-8-8 ou du patient mentionné au 2° du I de ce même article, tout ou partie des activités suivantes :

« 1° La mise à disposition et le maintien en condition opérationnelle des sites physiques permettant d'héberger l'infrastructure matérielle du système d'information utilisé pour le traitement des données de santé ;

« 2° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure matérielle du système d'information utilisé pour le traitement de données de santé ;

« 3° La mise à disposition et le maintien en condition opérationnelle de l'infrastructure virtuelle du système d'information utilisé pour le traitement des données de santé ;

« 4° La mise à disposition et le maintien en condition opérationnelle de la plateforme d'hébergement d'applications du système d'information ;

« 5° L'administration et l'exploitation du système d'information contenant les données de santé ;

« 6° La sauvegarde des données de santé.

« *Art. R. 1111-10.* – I. – Le certificat de conformité mentionné au II de l'article L. 1111-8 est délivré par un organisme de certification sur le fondement d'un référentiel de certification élaboré par le groupement d'intérêt public mentionné à l'article L. 1111-24 et approuvé par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés.

« II. – L'organisme de certification mentionné au II de l'article L. 1111-8 est accrédité par le Comité français d'accréditation ou par tout autre organisme d'accréditation signataire d'un accord de reconnaissance mutuelle multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation conformément à un référentiel d'accréditation élaboré par le groupement d'intérêt public mentionné à l'article L. 1111-24 en lien avec les organismes d'accréditation concernés et approuvé par arrêté du ministre chargé de la santé.

« III. – Le groupement d'intérêt public mentionné à l'article L. 1111-24 assure le suivi et la mise à jour de ces référentiels.

« *Art. R. 1111-11.* – I. – Le contrat d'hébergement mentionné au dernier alinéa du I de l'article L. 1111-8 est conclu entre l'hébergeur et son client. Il contient au moins les clauses suivantes :

« 1° L'indication du périmètre du certificat de conformité obtenu par l'hébergeur, ainsi que ses dates de délivrance et de renouvellement ;

« 2° La description des prestations réalisées, comprenant le contenu des services et résultats attendus notamment aux fins de garantir la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données hébergées ;

« 3° L'indication des lieux d'hébergement ;

« 4° Les mesures mises en œuvre pour garantir le respect des droits des personnes concernées par les données de santé dont notamment :

« – les modalités d'exercice des droits de portabilité des données ;

« – les modalités de signalement au responsable de traitement de la violation des données à caractère personnel ;

« – les modalités de conduite des audits par le délégué à la protection des données ;

« 5° La mention du référent contractuel du client de l'hébergeur à contacter pour le traitement des incidents ayant un impact sur les données de santé hébergées ;

« 6° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, le niveau garanti, la périodicité de leur mesure, ainsi que l'existence ou l'absence de pénalités applicables au non-respect de ceux-ci ;

« 7° Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau de protection équivalent de garantie au regard des obligations pesant sur l'hébergeur ;

« 8° Les modalités retenues pour encadrer les accès aux données de santé à caractère personnel hébergées ;

« 9° Les obligations de l'hébergeur à l'égard de la personne physique ou morale pour le compte de laquelle il héberge les données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ou imposées par le cadre légal applicable ;

« 10° Une information sur les garanties et les procédures mises en place par l'hébergeur permettant de couvrir toute défaillance éventuelle de sa part ;

« 11° La mention de l'interdiction pour l'hébergeur d'utiliser les données de santé hébergées à d'autres fins que l'exécution de l'activité d'hébergement de données de santé ;

« 12° Une présentation des prestations à la fin de l'hébergement, notamment en cas de perte ou de retrait de certification et les modalités de mise en œuvre de la réversibilité de la prestation d'hébergement de données de santé ;

« 13° L'engagement de l'hébergeur de restituer, à la fin de la prestation, la totalité des données de santé au responsable de traitement ;

« 14° L'engagement de l'hébergeur de détruire, à la fin de la prestation, les données de santé après l'accord formel du responsable de traitement et sans en garder de copie.

« II. – Lorsque le responsable de traitement de données de santé ou le patient mentionnés au I de l'article R. 1111-8-8 fait appel à un prestataire qui recourt lui-même pour l'hébergement des données à un hébergeur certifié, le contrat qui lie le responsable de traitement ou le patient avec son prestataire reprend les clauses mentionnées au I telles qu'elles figurent dans le contrat liant le prestataire et l'hébergeur certifié. »

Art. 3. – I. – L'ordonnance du 12 janvier 2017 susvisée et l'article 2 du présent décret entrent en vigueur le 1er avril 2018.

II. – Par dérogation au I, le 4° de l'article R. 1111-11 du code de la santé publique dans sa rédaction issue de l'article 2 du présent décret entre en vigueur le 25 mai 2018.

III. – Les agréments pour l'hébergement de données sur support numérique délivrés avant le 31 mars 2018 ou à la suite de demandes déposées avant cette date, restent régis jusqu'à leur terme par les dispositions de :

1° La sous-section 1 du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique dans leur rédaction avant l'entrée en vigueur de l'article 1er du présent décret ;

2° La sous-section 2 du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique dans leur rédaction avant l'entrée en vigueur de l'article 2 du présent décret.

IV. – Lorsque l'agrément pour l'hébergement de données de santé sur support informatique arrive à échéance avant le 31 mars 2019, la durée de l'agrément est prolongée pour une durée de six mois afin de permettre à l'hébergeur d'effectuer les démarches de certification nécessaires à la poursuite de son activité d'hébergement de données de santé.

Art. 4. – Avant le premier alinéa de l'article R. 1521-1 du code de la santé publique, il est inséré un alinéa ainsi rédigé :

« Les articles R. 1111-8-8 et R. 1111-9 à R. 1111-12 sont applicables aux îles Wallis et Futuna et aux Terres Australes dans leur rédaction issue du décret n° 2018-137 du 26 février 2018 »

Art. 5. – La ministre des solidarités et de la santé est chargée de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le 26 février 2018.

EDOUARD PHILIPPE

Par le Premier ministre :

La ministre des solidarités et de la santé,
AGNÈS BUZYN