RÉPUBLIQUE FRANÇAISE

Ministère des solidarités et de la santé

Décret n° 2017- …… du ……. relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique

NOR:

Publics concernés : *toute personne physique ou morale mentionnée à l'article L. 1111-8 qui héberge des données de santé, les prestataires qui concourent à la fourniture d'un service d'hébergement de données de santé, les organismes de certification, les responsables de traitement de données de santé à caractère personnel, les patients.*

Objet : *précision du périmètre de l'hébergement de données de santé prévu à l'article L. 1111-8 du code de la santé publique, mise en cohérence du code de la santé publique, définition de la procédure de certification pour l'hébergement de données de santé sur support numérique et de ses modalités d'entrée en vigueur.*

Entrée en vigueur *: les dispositions des articles 1 et 2 entrent en vigueur le lendemain de la publication du décret.*

Les dispositions de l'article 3 entrent en vigueur le 1er janvier 2018.

Notice : *le décret vise, d'une part, à adapter les dispositions du décret n° 2006-6 du 4 janvier 2006 aux modifications apportées par la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, et à appliquer les modifications apportées par l'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, à préciser le périmètre des activités d'hébergement de données de santé à caractère personnel soumises à agrément délivré par le ministre chargé de la santé ou à certification, et l'obligation pour toute personne physique ou morale à l'origine de la production ou du recueil desdites données de santé de recourir à un hébergeur certifié ou agréé dès lors qu'il externalise la conservation des données de santé 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 liste les clauses minimales que doit contenir le contrat d'hébergement de données de santé.

Enfin, le décret encadre la phase transitoire du maintien de la procédure d'agrément.

Références *: le présent décret ainsi que les textes qu'il modifie peuvent être consultés, dans leur rédaction résultant de cette modification, sur le site Légifrance (http://www.legifrance.gouv.fr).*

Le Président de la République,

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

Vu la directive 2006/123/CE du Parlement européen et du Conseil du 12 décembre 2006 relative aux services dans le marché intérieur ;

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, ensemble la notification XXX ;

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

Vu le code des relations entre le public et l'administration ;

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

Vu la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie, et notamment son article 137 ;

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

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

Vu le décret n° 97-34 du 15 janvier 1997 modifié relatif à la déconcentration des décisions administratives individuelles, notamment son article 2 ;

Vu le décret n° 97-1185 du 19 décembre 1997 modifié pris pour l'application à la ministre de l'emploi et de la solidarité du 1° de l'article 2 du décret du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel ;

Vu le décret n° 2008-1326 du 15 décembre 2008 relatif au dossier pharmaceutique ;

Vu le décret n° 2008-1401 du 19 décembre 2008 relatif à l'accréditation et à l'évaluation de conformité pris en application de l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie ;

Vu le décret n°2009-697 du 16 juin 2009 relatif à la normalisation, notamment son article 17 ;

Vu le décret 2011-246 du 4 mars 2011 relatif à l'hébergement de données de santé à caractère personnel sur support papier ;

Vu le décret n° 2016-914 du 4 juillet 2016 relatif au dossier médical partagé ;

Vu l'avis du Conseil national de l'ordre des médecins en date du_____;

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

Vu l'avis du Conseil national de l'ordre des pharmaciens en date du _____ ;

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

Vu l'avis du Conseil national de l'ordre des infirmiers en date du _____ ;

Vu l'avis du Conseil national de l'ordre des masseurs-kinésithérapeutes en date du _____ ;

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

Vu l'avis de la Commission nationale de l'informatique et des libertés en date de _____ ;

Le Conseil d'Etat (section sociale) entendu ;

Le Conseil des ministres entendu,

Article 1

I. La sous-section 1 de la section 1 du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique est ainsi modifiée :

1° A l'article R. 1111-1, au premier alinéa, les mots : « professionnel de santé, un établissement de santé ou un hébergeur agréé » 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° A l'article R. 1111-2, au premier alinéa, 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° A l'article R. 1111-3, au premier alinéa, 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.

II. 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, un hébergement temporaire de données n'ayant pas pour finalité d'organiser leur accès ou leur transmission au profit du responsable de traitement, du patient ou de tout professionnel participant à la prise en charge de la personne concernée par les données.

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

III. 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 ainsi modifiée :

1° Au dernier alinéa de l'article R*.1111-10, les mots : « de rejet » sont remplacés par les mots : « d'acceptation » ;

2° 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 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 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 articles L.1110-4 et L.1110-4-1;

3° L'article R.1111-14 est ainsi modifié :

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 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. ».

Article 2

I. La section 2 bis du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique est ainsi modifiée :

1° A l'article R. 1111-20-4, au deuxième alinéa, 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 ;

2° A l'article R. 1111-20-10, les mots : « agréé en application des articles R. 1111-9 à R. 1111-16 » sont remplacés par les mots : « dans le respect de l'article L.1111-8» ;

3° Au 2°, 3° a et 3° b de l'article R.1111-20-11 les mots : « l'hébergeur détruit les données, ainsi que les traces d'interventions mentionnées au II de l'article R. 1111-20-2. » sont remplacés par les mots : « les données, ainsi que les traces d'interventions mentionnées au II de l'article R. 1111-20-2 sont détruites. » ;

4° Le 3° de l'article R. 1111-35 est remplacé par les mots : « 3° Par l'intermédiaire de la Caisse nationale de l'assurance maladie des travailleurs salariés. ».

II. Le chapitre II du titre Ier du livre Ier de la première partie du code de la santé publique est ainsi modifié : à 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 de l'article L.1111-8. ».

III. Le chapitre VI du titre Ier du livre III de la première partie du code de la santé publique est ainsi modifié : à 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.

Article 3

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. Toute personne physique ou morale assurant une activité d'hébergement sur support numérique de données de santé à caractère personnel mentionnées au I de l'article R.1111-8-8, doit être titulaire d'un certificat de conformité délivré par un organisme de certification accrédité pour la certification relative à l'hébergement de données de santé, par le Comité français d'accréditation ou l'instance nationale d'accréditation d'un autre Etat membre de l'Union européenne membre de la coopération européenne pour l'accréditation et ayant signé les accords de reconnaissance mutuelle multilatéraux couvrant la certification considérée.

« L'organisme de certification est accrédité 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.

« Le certificat de conformité mentionné au II de l'article L. 1111-8 est délivré 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.

« Sous réserve de sa conformité aux conditions prévues par le présent article, l'organisme de certification est librement choisi par l'hébergeur. »

« Art. R. 1111-11. Le contrat d'hébergement mentionné au dernier alinéa du I de l'article L. 1111-8, 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 ;
« 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 détruire les données de santé, sans en garder copie en fin de prestation.

« Le contrat d'hébergement est conclu entre l'hébergeur certifié et son client.

« 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 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 précitées telles qu'elles figurent dans le contrat liant le prestataire et l'hébergeur certifié. »

« Art. R. 1111-12. Le groupement d'intérêt public mentionné à l'article L. 1111-24 est chargé d'établir et de participer au développement de la procédure de certification des hébergeurs de données de santé sur support numérique. Il assure également le suivi du référentiel d'accréditation en lien avec les organismes d'accréditation concernés et le suivi et la mise à jour du référentiel de certification. »

Article 4

I. L'ordonnance n° 2017-27 du 12 janvier 2017 entre en vigueur le 1er janvier 2018.

II. L'article 3 du présent décret entre en vigueur le 1er janvier 2018.

III. La sous-section 1 du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique dans sa rédaction antérieure au présent décret et la sous-section 2 du chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique dans sa rédaction résultant du III de l'article 1er du présent décret demeurent applicables :

1°) Aux agréments délivrés avant le 1er janvier 2018 pour l'hébergement de données sur support électronique ;

2°) Aux agréments délivrés après cette date pour des demandes déposées jusqu'au 31 décembre 2017.

IV. Lorsque l'agrément pour l'hébergement de données de santé sur support électronique arrive à son terme dans les douze mois suivants l'entrée en vigueur de la procédure de certification, 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.

Article 5

L'article 3 du présent décret est applicable, aux îles Wallis et Futuna et aux Terres Australes.

Article 6

Le Premier ministre, le ministre de l'économie et la ministre des solidarités et de la santé sont responsables, chacun en ce qui le concerne, de l'application du présent décret, qui sera publié au Journal officiel de la République française.

Fait le

Par le Premier ministre :

Le ministre de l'économie

La ministre des solidarités et de la santé