L'hébergement de données de santé : une procédure assouplie pour une plus grande responsabilité des acteurs

La nouvelle procédure de certification des hébergeurs de données personnelles de santé qui remplacera demain l'agrément actuel consacre l'importance du sujet de la sécurité des bases de données de santé et acquiert désormais une dimension européenne en accord avec l'esprit du Règlement européen sur la protection des données personnelles.

Par **JEANNE BOSSI MALAFOSSE,**
Avocat associé DELSOL Avocats

En application de l'article 204 de la loi du 26 janvier 2016 de modernisation de notre système de santé et de l'ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel, la procédure d'agrément des hébergeurs de données de santé sera remplacée à compter du 1er janvier 2018 par une procédure de certification[1].

La procédure d'agrément actuelle, mise en place effectivement en 2009 par l'Agence des systèmes d'information partagés de santé (ASIP Santé) à la demande du ministère chargé de la santé qui fait intervenir un comité d'agrément des hébergeurs (CAH) et la CNIL, va disparaître au profit d'un mécanisme de certification délivré par un organisme certificateur accrédité par le Comité français d'accréditation (Cofrac). Cette certification pourra également être délivrée par l'organisme compétent d'un autre Etat membre de l'Union européenne.

L'hébergement des données de santé doit permettre d'**organiser le dépôt et la conservation des données personnelles de santé dans des conditions de nature à en garantir leur pérennité et leur confidentialité,** de les mettre à la disposition des personnes autorisées selon des modalités définies par contrat et de les restituer en fin de contrat.

La certification est une procédure par laquelle une tierce partie (externe) donne l'assurance écrite qu'un produit, processus, service ou compétence est en conformité avec certaines normes.

En fondant désormais la reconnaissance de la qualité d'hébergeur de données personnelles de santé sur le respect de normes techniques fondées sur des standards internationaux du secteur - orientation impossible à prendre en 2009 qui marquait le début des travaux concertés sur les référentiels de sécurité - les pouvoirs publics poursuivent leur action destinée à définir une Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSIS).

Ce passage d'une autorisation à un mécanisme de certification, mécanisme volontaire et accessible via un processus transparent, s'intègre également dans un mouvement plus général qui vise à responsabiliser les acteurs impliqués dans le traitement de données à caractère personnel. Il rejoint ainsi l'esprit porté par le nouveau Règlement européen sur la protection des données personnelles (RGPD) du 27 avril 2016 qui place le principe d'accountability au cœur de son application.

La certification donne l'assurance écrite qu'un produit, processus, service ou compétence est en conformité avec une norme

La nouvelle procédure de certification, prenant en compte les enseignements de l'agrément est **plus adaptée aujourd'hui aux nouveaux systèmes d'information et revêt désormais une dimension européenne** qui s'accorde avec l'esprit du nouveau Règlement européen sur la protection de données personnelles.

LE PASSAGE DE L'AGRÉMENT À LA CERTIFICATION

• **La procédure de l'agrément a contribué à élever le niveau de sécurité**

Le principe de l'agrément dans le domaine de l'hébergement des données de santé a été posé par la loi n° 2002- 303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé des malades à l'époque où les premières bases de données de santé se développaient sur internet. Appelé de ses vœux par la CNIL[2], cet encadrement visait à garantir la confidentialité des données de santé conservées par des entités qui s'interfaçaient ainsi entre les patients et les professionnels de santé posant clairement la question du respect du secret médical.

Les conditions d'obtention de l'agrément ont ensuite été fixées par le décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique.

La prestation d'hébergement est un contrat dont le contenu est fixé précisément

Les articles R1111-9 à R1111-16 du code de la santé publique décrivent une procédure et des exigences faisant intervenir un Comité d'Agrément des Hébergeurs (CAH) composé de huit membres titulaires[3] désignés par arrêté, chargé, après instruction des dossiers par les agents de l'ASIP Santé pour le compte du ministère chargé de la santé, d'émettre un avis destiné à être transmis au ministre, seul habilité à prononcer l'agrément. La procédure fait également intervenir la CNIL qui doit émettre un avis sur le dossier qui lui aura été préalablement transmis par l'ASIP Santé.

Appliquée une première fois aux premières expérimentations du Dossier Médical Personnel en 2006 puis suspendue pendant deux ans, la procédure d'agrément, a été effectivement mise en place par l'Agence des Systèmes d'Information de Santé (ASIP Santé) en 2009. **Elle concerne l'hébergement des données recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins confiées par des professionnels de santé ou des établissements de santé ou la personne concernée.**

La prestation d'hébergement est un contrat dont le contenu est fixé précisément à l'article R1111-13 du code de la santé publique. L'agrément repose sur l'évaluation de la capacité financière du candidat, l'appréciation du niveau de sa politique de sécurité au regard d'un référentiel affiché et arrêté en concertation avec l'ensemble des acteurs institutionnels et industriels du secteur et la vérification des mesures mises en place pour assurer le respect des droits de la personne concernée[4].

L'agrément est délivré pour trois ans par le ministre chargé de la santé et jusqu'à présent la présence chez l'hébergeur d'un médecin, garant du secret professionnel est exigée.

La consécration au niveau législatif de cette procédure et de son caractère obligatoire a été essentielle pour fonder sa légitimité et reconnaître le rôle essentiel tenu par les autorités et instances susvisées[5].

Cette procédure a incontestablement permis d'élever le niveau de sécurité des bases de données de santé souvent, pour certaines d'entre elles, très peu sécurisées. Elle a surtout été construite en concertation avec les acteurs en se fondant sur des référentiels techniques et de sécurité à l'état de l'art devenus des références communes pour tous les acteurs.

Elle a pu ainsi conduire les hébergeurs vers un état de l'art dépendant des progrès technologiques dont ils sont eux-mêmes souvent les instigateurs[6]. Mais cette procédure reste indubitablement complexe et longue[7]

et la multiplication du nombre des dossiers est devenu difficilement compatible avec la conduite de projets de plus en plus nombreux à recourir à l'hébergement, devenu un élément essentiel de la nouvelle urbanisation des systèmes d'information de santé.

La loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé est venue clarifier certains aspects de cette procédure et surtout, annoncer son évolution vers un processus de certification.

- **La certification est aujourd'hui plus adaptée au contexte des systèmes d'information partagés**

L'ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel annoncée par la loi précitée du 26 janvier 2016 définit un nouveau champ d'application de l'hébergement des données de santé et annonce une nouvelle procédure fondée sur la certification des hébergeurs[8].

La prestation d'hébergement doit faire l'objet d'un contrat et la personne concernée doit être dûment informée

L'ordonnance modifie l'article L. 1111-8 du code de la santé publique qui prévoit désormais que *« Toute personne qui héberge des 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, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données ou pour le compte du patient lui-même, réalise cet hébergement dans les conditions prévues au présent article. ».*

Il est rappelé que la prestation d'hébergement doit faire l'objet d'un contrat et que la personne concernée doit être dûment informée et en mesure de s'opposer à l'hébergement sur support papier ou numérique de ses données.

L'hébergeur des données précitées sur support numérique doit être titulaire d'un certificat de conformité.

Le nouvel article L1111-8 du code de la santé publique renvoie à un décret en Conseil d'Etat pris après avis de la CNIL et des conseils nationaux de l'ordre des professions de santé, le soin de :
- fixer les conditions de délivrance du certificat et,
- préciser la nature des prestations d'hébergement, les rôles et responsabilités de l'hébergeur et des personnes physiques ou morales pour le compte desquelles les données de santé à caractère personnel sont conservées, ainsi que les stipulations devant figurer dans le contrat d'hébergement.

Le projet de décret annoncé ainsi que le projet d'arrêté visé à l'article 3 du projet de décret précité portant approbation du référentiel d'accréditation des organismes de certification et du référentiel de certification pour l'hébergement de données de santé à caractère personnel ont fait l'objet pendant l'été 2017 d'une procédure de consultation auprès de la Commission Européenne (cf ci-dessous).

Sur le champ d'application de l'hébergement

Le projet de décret précise que l'activité d'hébergement ne se limite plus aux seules données recueillies à l'occasion des activités de prévention, de diagnostic ou de soins mais inclut désormais celles recueillies à l'occasion d'activités : *« … de suivi social et médico-social ».*

Cette rédaction s'articule ainsi avec les nouvelles dispositions qui définissent le cadre juridique de l'échange et du partage des données de santé à caractère personnel désormais articulé autour de la définition d'une équipe de soins élargie (article L1110-12 du code de la santé publique), respectueuse de la vie privée des personnes (article L1110-4 du code de la santé publique), et des référentiels de sécurité et d'interopérabilité opposables (article L1110-4-1 du code de la santé publique).

Le parcours de soins du patient implique en effet aujourd'hui l'intervention d'une équipe de soins issue d'organisations diverses et élargie aux professionnels du

secteur médico-social et social. Ces acteurs utilisent des systèmes d'information qui recourent pour la plupart du temps à l'hébergement et qui, personnes physiques ou morales à l'origine du dépôt des données auprès de l'hébergeur, restent responsables de traitement au sens de l'article 3 de la loi Informatique et Libertés.

Concernant l'utilisation des données, l'ordonnance rappelle que les hébergeurs ont "*l'interdiction d'utiliser les données à d'autres fins que l'exécution de la prestation d'hébergement*" et qu'ils doivent restituer les données aux personnes qui les leur ont confiées "*sans en garder copie*" lorsqu'il est mis fin à l'hébergement. Tout acte de cession à titre onéreux des données hébergées, y compris avec l'accord de la personne concernée est par ailleurs interdite.

Le contrat d'hébergement

Les obligations précitées sont reprises dans le contrat qui lie le responsable de traitement et l'hébergeur et dont le contenu est prévu au nouveau projet d'article R1111-13 du projet de décret.

Devront ainsi notamment être indiqués dans le contrat le périmètre du certificat obtenu, les lieux d'hébergement des données, 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, une information sur le recours à d'éventuels prestataires techniques.

Le contrat est conclu entre l'hébergeur certifié et le client. Le projet de décret indique que pour les cas où le client, qu'il soit la personne concernée ou le responsable de traitement qui produit ou recueille les données de santé, recourt aux services d'un prestataire qui lui-même fait héberger les données, alors les clauses énumérées dans le projet d'article précité doivent être reprises dans le contrat avec le prestataire.

L'ordonnance rappelle également, comme c'était déjà le cas auparavant, que les hébergeurs et les personnes placées sous leur autorité qui ont accès aux données déposées sont astreints au secret professionnel dans les conditions et sous les peines prévues à l'article 226-13 du code pénal.

Une période de transition prévue

Une période de transition entre l'agrément et la certification est prévue à l'article 3 de l'ordonnance n° 2017-27 du 12 janvier 2017 dont les dispositions entreront en vigueur le 1er janvier 2018. Les hébergeurs ayant déjà obtenu l'agrément HDS conservent cet agrément jusqu'à son échéance. Ce n'est qu'à l'issue de celle-ci qu'ils devront obtenir une certification. Dans les cas où le terme de l'agrément obtenu arrive à échéance dans les douze mois suivants le 1er janvier 2018, celui-ci est prolongé de six mois pour permettre à l'hébergeur d'obtenir un certificat de conformité.

Toutes les demandes d'agrément déposées avant le 31 décembre 2017 resteront régies par les dispositions précédant l'ordonnance de 2017.

LA PROCÉDURE DE LA CERTIFICATION, NOUVEL OUTIL DE CONFORMITÉ À L'ÉCHELLE EUROPÉENNE

- **La nouvelle procédure de certification**

L'ordonnance du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel dispose que l'hébergeur devra être détenteur d'un certificat de conformité délivré par : … *« des organismes de certification accrédités par l'instance française d'accréditation ou l'instance nationale d'accréditation d'un autre Etat membre de l'Union européenne mentionnée à l'article 137 de la loi n°2008-776 du 4 août 2008 de modernisation de l'économie ».*

Un projet de décret définit les conditions de délivrance de ce certificat.

L'organisme de certification est accrédité sur le fondement d'un référentiel d'accréditation élaboré par l'ASIP Santé en lien avec les organismes d'accréditation concernés et approuvé par arrêt du ministre chargé de la santé. La certification elle-même interviendra sur la base d'un référentiel de certification également élaboré par l'ASIP Santé et approuvé par le ministre chargé de la santé après avis de la CNIL.

L'ASIP Santé poursuit ainsi son rôle d'initiateur et de coordinateur pour cette nouvelle procédure puisque le projet de décret indique que l'agence est chargée : *« … d'établir et de participer au développement de la procédure de certification des hébergeurs de données de santé sur support numérique »* et qu'elle doit en outre assurer le suivi du référentiel d'accréditation et sa mise à jour.

Le projet de décret procède à la description du type d'activités caractérisant l'activité de l'hébergeur (projet d'article R 1111-9) :

- *« 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. »*

D'ores et déjà, deux types de certificats sont identifiés comme pouvant être délivrés aux hébergeurs, correspondant à deux métiers d'hébergement distincts :

- **un certificat « hébergeur d'infrastructure physique »** pour les activités de mise à disposition de locaux d'hébergement physique et d'infrastructure matérielle ;

- **un certificat « hébergeur infogéreur »** pour les activités de mise à disposition d'infrastructure virtuelle, de mise à disposition de plateforme logicielle, d'infogérance et de sauvegarde externalisée.

Le référentiel de certification annexé au projet d'arrêté est fondé sur des normes internationales : la norme ISO 27001 relative au système de gestion de la sécurité des systèmes d'information dont le respect sera obligatoire ; le respect d'exigences de la norme ISO 20000 relative au système de gestion de la qualité des services et le respect d'exigences de la norme ISO 27018 sur la protection des données personnelles et de la norme ISO 27017 plus axée sur les aspects de la sécurité de l'information du *cloud computing*.

Il est important de noter que d'autres exigences propres à l'activité d'hébergement pourront également être identifiées mais elles ne sont pas connues à ce jour.

La procédure elle-même de certification sera classique et consistera en un audit documentaire et un audit sur site.

Le certificat sera délivré pour trois ans par l'organisme certificateur et un audit de surveillance annuel sera effectué.

- **L'environnement européen**

Il est intéressant de noter que cette nouvelle procédure de certification prévoit la possibilité qu'un organisme certificateur puisse être accrédité non seulement par le COFRAC français mais également par l'instance nationale d'accréditation d'un autre Etat membre.

Ce point est important dans la mesure où jusqu'à présent la procédure d'agrément pour l'hébergement restait une spécificité française. La référence à des normes ISO internationales et l'intervention possible d'une instance d'accréditation autre que le COFRAC constituent des éléments qui confèrent à cette nouvelle procédure une dimension européenne et internationale.

La note d'information publiée sur le site de la Commission européenne précise en effet que cette nouvelle procédure permet de prendre en compte le caractère potentiellement international de l'hébergement (prestataire d'hébergement de droit international, activité d'hébergement exercée en dehors du territoire national).

Notons toutefois que la procédure d'agrément française avait déjà acquis au cours des dernières années une notoriété certaine puisque de nombreux groupes industriels souhaitant développer des services en France ont dû obtenir l'agrément.

L'exposé des motifs qui accompagne le projet de décret notifié à la Commission européenne précise que cette certification doit permettre *« de garantir aux personnes physiques le respect de leur vie privée et du secret médical. Elle est de nature à diminuer le risque de violation des données à caractère personnel en renforçant les conditions de leur hébergement »*.

Cette nouvelle procédure sera donc plus compétitive. En effet, elle permettra à des entreprises d'obtenir une certification dans un autre Etat membre là où hier, seul le recours à l'obtention de l'agrément était possible pour l'hébergement des données de santé en France. La procédure rejoint ainsi le domaine des certifications

déjà existantes dans le secteur d'activité de l'hébergement des données à caractère personnel. En effet, le secteur de la santé connait déjà d'autres procédures de certification à l'échelle européenne. C'est notamment le cas pour les dispositifs médicaux qui peuvent faire l'objet d'un certificat CE préalablement à leur mise en circulation, auprès de n'importe quel organisme certificateur compétent dans les Etats membres concernés.

Cette procédure traduit également une tendance bénéfique à l'uniformisation des procédures à l'échelle européenne mettant ainsi en œuvre l'esprit du Règlement européen sur la protection des données personnelles (RGPD) et les outils qu'il propose[9].

Le RGPD met en avant le principe d'accountability tourné vers une plus grande responsabilisation des acteurs du traitement de données à caractère personnel. Ce principe se traduit notamment par la suppression des formalités préalables au profit de l'obligation pour le responsable de traitement et le sous-traitant de démontrer leur conformité aux principes de protection des données personnelles.

Le RGPD met à la disposition des acteurs, responsables de traitement et sous-traitants, de nouveaux outils de conformité, tels que la certification, les codes de conduite, les labels consacrant ainsi le recours aux outils de *soft law.*

L'intégration de ces outils par le Règlement européen de protection des données personnelles permet de développer des outils à l'échelle européenne et ainsi de garantir une application uniforme du Règlement tout en continuant à responsabiliser les acteurs par des mécanismes transparents et applicables à tous sur une base volontaire. L'exposé des motifs accompagnant les projets de décret et d'arrêté, soumis à consultation sur le site de la Commission européenne, est également intéressant quand il rappelle que la procédure de certification *« s'inscrit pleinement dans l'esprit du 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, qui préconise la mise en place de mécanisme de certification ».*

Les responsables de traitement et les sous-traitants devront dès l'origine concevoir l'ensemble de leurs projets en intégrant les principes de protection des données personnelles. Ainsi, dans le cadre d'un projet qui implique l'hébergement de données de santé, il sera obligatoire, dès la conception du système, de veiller à respecter le référentiel adopté et les conditions d'hébergement de ces données.

La prestation d'hébergement de données de santé étant toujours définie dans un contrat, dont le contenu est défini au nouveau projet d'article R. 1111-11 du code de la santé publique, il devra également être établi conformément aux dispositions du RGPD qui précise et renforce les obligations des sous-traitants (article 28 du RGPD). Les obligations du Règlement relatives à la relation entre responsable de traitement et sous-traitant devront donc également être prises en compte dans le contrat d'hébergement.

EN CONCLUSION

La transformation du cadre juridique relatif à l'hébergement des données personnelles de santé intervient à un moment important pour les acteurs : d'abord parce qu'elle consacre la maturité acquise sur le sujet grâce aux enseignements de la procédure d'agrément qui a permis, au-delà de l'urgence qu'il y avait à encadrer une activité alors émergente et sensible, de définir un politique de sécurité adaptée ; ensuite parce qu'elle intervient à la veille de l'entrée en application du Règlement européen sur la protection des données personnelles dont l'esprit fondé sur la responsabilisation des acteurs retient l'idée de la certification.

Il restera à chaque acteur à intégrer le respect des droits de la personne, sujet un peu passé sous silence par les débats sur la nouvelle certification des hébergeurs mais qui reste un des fondements initial de l'encadrement de l'activité d'hébergement et qui, avec le nouveau Règlement européen doit être au centre des préoccupations des acteurs, les sanctions encourues en cas de non-respect des droits de la personne étant plus lourdes que celles applicables au non-respect d'exigences techniques.

RÉFÉRENCES

1 Le projet de décret pris en application de l'ordonnance du 12 janvier 2017 qui a été notifié à la Commission Européenne annonce en effet la date du 1er janvier 2018 pour la mise en œuvre de la nouvelle procédure de notification.

2 Délibération n°01-011du 8 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au public.

3 Sont également désignés huit membres suppléants.

4 Référentiel d'agrément accessible sur esante.gouv.fr. Le consentement de la personne concernée initialement exigé par la loi a été supprimé par la loi n°2016-41 du 26 janvier 2016.

5 96 dossiers ont été agréés à la date du 18 octobre 2017 et près de 40 % des dossiers déposés n'ont pas été agréés ou l'ont été à l'issue d'un deuxième examen.

6 Nouvelles offres intégrant le cloud computing, développement de solutions de mobilité, etc…

7 Délai moyen de huit mois pour obtenir l'agrément, nécessité d'actualiser son agrément tous les ans, et de le renouveler tous les trois ans après réalisation d'un audit.

8 Hors service d'archivage électronique (article L1111-8 III du code de la santé publique).

9 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)