Certification des hébergeurs de données de Santé et décret n° 2018-137 du 26 février 2018

L'hébergement de données de santé à caractère personnel : de l'agrément à la certification des hébergeurs (suites).

On rappellera d'abord que, dans le prolongement de la loi dite « Touraine », n° 2016-41 du 26 janvier 2016 relative à la modernisation de notre système de Santé, une Ordonnance n° 2017-27 en date du 12 janvier 2017 a modifié une obligation juridique qui intéresse les SSTI concernant l'hébergement de données à caractère personnel.

En effet, s'agissant de l'hébergement des données de santé, nombre de SSTI ont contracté avec des structures agréées à cet effet et listées en conséquence par l'ASIP.

Or, le principe et les modalités de l'agrément en la matière sont modifiés et, à compter du 1er janvier 2019, c'est un mécanisme de certification qui est mis en place.

De plus, le libellé du nouvel article L. 1111-8 du Code de la Santé publique permet de conclure que les Services eux-mêmes vont avoir à obtenir une telle certification.

En effet, cet article est ainsi rédigé :

« 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. »

On relèvera donc que la loi ne vise plus, comme précédemment, le seul dépôt de données de Santé auprès d'hébergeurs agréés par la personne concernée, mais oblige toute personne qui héberge de telles données recueillies à l'occasion d'activités de prévention, notamment, « *dès lors qu'elles le sont pour le compte des personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou encore de la personne suivie elle-même* ».

Cette nouvelle rédaction, élargie, implique, selon Présanse, que tout Service réponde à l'obligation de certification nouvellement révisée.

En complément de l'article publié dans les Informations Mensuelles n° 67 page 5, explicitant le changement du régime applicable – lequel passe donc de l'agrément de l'hébergeur concerné à sa certification, on rappellera ici que le certificat de conformité envisagé par les textes doit s'appuyer sur un référentiel et que l'ASIP a déjà publié un « *référentiel de certification des hébergeurs de données de santé* » sur son site.

C'est dans ce contexte que le décret n° 2018-137 du 26 février 2018 relatif à l'hébergement de données de santé à caractère personnel a été publié au J.O du 28 février 2018.

Il y est précisé le champ des activités d'hébergement de ces données et fixé celles qui nécessitent désormais une certification, ainsi que les modalités de ce régime.

On observera, en outre, que ces dispositions sont notamment élaborées sous le visa du RGPD.

On précisera ensuite, qu'il est inséré dans le Code de la Santé publique, une sous-section 1 ter ainsi rédigée :

« 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. »

Le libellé de cette disposition réglementaire, reprenant le principe posé par la loi, semble bien confirmer que les SSTI sont concernés.

De plus, il est désormais indiqué :

« 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. »

Le contrat d'hébergement fait ensuite l'objet de dispositions spécifiques, obligeant à l'élaboration de clauses relatives, notamment, aux mesures visant à garantir le respect des droits des personnes concernées par ces données de Santé.

Enfin, le décret explicite les dates d'application dans le temps du nouveau régime de certification créé et énonce à ce titre que les agréments délivrés avant le 31 mars prochain restent soumis au régime antérieur jusqu'à leur terme et que ceux qui arrivent à échéance avant le 31 mars 2019 seront prolongés de 6 mois pour permettre les démarches de certification. En pratique, les contrats d'hébergement existants vont donc être modifiés pour se conformer aux nouvelles dispositions et les Services vont avoir à initier une démarche de certification dédiée aux données de Santé à caractère personnel qu'ils hébergent dans le cadre de l'exécution de leur mission. ■