

# Données de santé : ce que change la loi du 26 janvier 2016

JURIDIQUE, SANTÉ, DONNÉES PERSONNELLES

PUBLIÉ LE 29 JANVIER 2016 À 16H47

TWITTER

FACEBOOK

LINKEDIN

GOOGLE +

La procédure d'agrément des hébergeurs de données de santé à caractère personnel vient d'être entièrement refondée par la loi de modernisation de notre système de santé du 26 janvier 2016 au bénéfice d'une procédure de certification.



Protected design - INPI N°10/3563

Données de santé : ce que change la loi du 26 janvier 2016

© Withings

La loi de modernisation de notre système de santé n°2016-41 vient d'être promulguée le 26 janvier 2016 et publiée au jour janvier 2016.

Rappelons que la procédure d'agrément des hébergeurs de données de santé à caractère personnel a été instaurée par la loi n°2002-276 du 4 mars 2002, dite "loi Kouchner". Elle vise à assurer la sécurité, la confidentialité et la disponibilité des données de santé à caractère personnel, lorsque leur hébergement est externalisé.

## DE L'HÉBERGEMENT DE DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL

Pilotée par l'ASIP Santé, elle s'impose dans les conditions suivantes : "Les professionnels de santé ou les établissements de santé ou toute autre personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion de la prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement ne peut avoir lieu qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée" (Article L1111-8 du Code de la Santé Publique).

Selon l'interprétation pragmatique de l'ASIP Santé, la réglementation (art. L1111-8 et R1111-9 à 14 CSP) s'applique à tout traitement, au sens de la loi Informatique et libertés n°78-17 du 6-1-1978 qui externalise l'hébergement des données de santé à caractère personnel qu'il traite, incluant notamment les mutuelles et assurances. L'agrément est délivré après instruction (8 mois maximum) remis par le candidat à l'ASIP Santé, s'articulant autour de 6 principaux formulaires détaillant les caractéristiques techniques et économiques de la prestation d'hébergement.

[D'après l'ASIP Santé](#), le candidat à l'agrément doit couvrir l'ensemble des obligations réglementaires, par lui-même ou en collaboration avec un sous-traitant, et s'adresser expressément certaines sur son client ou ses sous-traitants, dans le cadre du contrat d'hébergement ou du/des contrat(s)

## UNE ÉVALUATION DE CONFORMITÉ TECHNIQUE REMPLACE L'AGRÉMENT

La loi de janvier 2016 modifie substantiellement l'art. 1111-8 CSP. Son article 96 I 5° a) prévoit ainsi : "Toute personne qui donne des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou le patient lui-même, doit être agréée à cet effet. Cet hébergement, quel qu'en soit le support, papier ou électronique, est réalisé par une personne prise en charge en a été dûment informée et sauf opposition pour un motif légitime".

Cette nouvelle formulation étend le périmètre de l'obligation, pour les responsables de traitement, en cas d'externalisation ou de recours à un hébergeur agréé, dès lors qu'elle s'impose dorénavant au secteur de la santé, mais aussi à celui du secteur privé. En outre, ailleurs, le consentement de la personne concernée par les données - dûment informée - n'a plus à être recueilli : il est prévu à l'article 204 I 5° c) de la loi habilite le gouvernement, par voie d'ordonnance, dans un délai d'1 an à compter de la promulgation de la loi, de remplacer l'agrément par une "évaluation de conformité technique".

### 3 TYPES DE CERTIFICATION

L'ASIP Santé a anticipé sur la procédure de certification et segmenté les services des hébergeurs. Elle envisage 3 types de certification :

- **Hébergeur d'infrastructure**, incluant la fourniture de l'hébergement physique ainsi que la mise en œuvre des matériels informatiques, leur maintenance, et éventuellement l'activité de sauvegardes externalisées
- **Infogérance d'hébergement**, incluant l'activité d'infogérance hors infogérance de l'application métier, et éventuellement l'activité de sauvegardes externalisées
- **Hébergeur de données de santé**, regroupant les deux premières certifications.

Ainsi, tous les acteurs de la chaîne seraient désormais certifiés pour leur périmètre de responsabilités, à l'exclusion du périmètre de son client ou de ses sous-traitants. De la sorte, les contrats d'hébergement et de sous-traitance n'auront plus à intégrer les reports d'obligations à leur égard et s'en trouveront donc largement simplifiés.

### CERTIFICATION POUR 3 ANS

Les hébergeurs seraient désormais certifiés pour 3 ans par un organisme certificateur, lui-même accrédité par un organisme de certification pour 5 ans (en France, le COFRAC).

La nouvelle procédure de certification serait mise en place après la publication de l'ordonnance du gouvernement et aussi celle de l'ASIP Santé, soit à une échéance de 2 ans à compter de la promulgation de la loi le 26 janvier 2016.

Les agréments en vigueur à cette date devraient rester valables jusqu'à leur terme.

**Marguerite Brac de la Perrière, Aude Latrive, avocats, cabinet Alain Bensoussan Avocats**

#### Recommandations :

- Anticiper sur le périmètre de certification de l'agrément par sa prestation d'hébergement
- Mettre en conformité sa prestation avec la norme ISO27001, qui sera exigée pour la nouvelle certification
- S'il était confirmé que les agréments existants à la date de mise en place de la nouvelle certification le restaient jusqu'à leurs termes, prévoir le renouvellement des agréments