PREMIER RAPPORT D'ACTIVITÉ

DU COMITÉ D'AGRÉMENT DES HÉBERGEURS : 2006-2011,

sous la présidence du Docteur Philippe BICLET

INTRODUCTION 4

TITRE 1 : L'ENCADREMENT DE L'HEBERGEMENT DES DONNEES DE SANTE A CARACTERE PERSONNEL **4**
A- LE CADRE JURIDIQUE ET LE PERIMETRE DE L'HEBERGEMENT DE DONNEES DE SANTE A CARACTERE PERSONNEL 5
B- LA NOTION D'HEBERGEMENT 5
TITRE 2 : LE DEROULEMENT DE LA PROCEDURE D'AGREMENT DES HEBERGEURS DE DONNEES DE SANTE A CARACTERE PERSONNEL **6**
A- LES ACTEURS DE LA PROCEDURE D'AGRÉMENT 6
1) Le candidat 6
2) La Commission nationale de l'informatique et des libertés (CNIL) 6
3) Le Comité d'agrément 6
4) Le Ministre chargé de la santé 7
5) L'Agence des systèmes d'information partagés de santé (ASIP Santé) 7
B- LE DEROULEMENT DE LA PROCEDURE 8
1) La réception du dossier de demande d'agrément 8
2) L'instruction du dossier par l'ASIP Santé et la CNIL 8
TITRE 3 : L'ACTIVITE DU COMITE D'AGREMENT **9**
A- UN PREMIER BILAN GLOBALEMENT POSITIF 9
B- LA QUESTION DE LA RECEVABILITE DES DEMANDES D'AGREMENT : ELEMENT CLE DE LA PROCEDURE 11
TITRE 4 : ARTICULATION DES EXPERTISES DU COMITE D'AGREMENT ET DE LA CNIL **14**
A- LA CNIL DANS LA PROCEDURE D'AGREMENT 14
B- L'HOMOGENEITE DE LA DOCTRINE DU COMITE D'AGREMENT ET DE LA CNIL 17
TITRE 5 : LA DOCTRINE PROPRE AU COMITE D'AGREMENT **18**
A- LES CARACTERISTIQUES DU DOSSIER DE DEMANDE D'AGREMENT 18
1) Le candidat 18
2) Le client 19
3) La personne concernée par les données hébergées (le patient) 19
4) Le médecin de l'hébergeur 19
B- LE CONTRAT D'HEBERGEMENT 21
C- LE CONTRAT AVEC LES SOUS-TRAITANTS 22
D- BILAN ECONOMIQUE ET FINANCIER 23
E- RECOMMANDATIONS PERMETTANT AUX CANDIDATS DE MIEUX PRESENTER LES ASPECTS SECURITE ET TECHNIQUE 23
F- LES SUITES DE L'AGREMENT 25
TITRE 6 : BILAN ET PERSPECTIVES **25**
TITRE 7 : CONCLUSION **27**
LES RECOMMANDATIONS DU COMITE D'AGREMENT EN 8 POINTS 29
LE POINT DE VUE DE NATHALIE TELLIER, MEMBRE DU COMITE D'AGREMENT AU TITRE DES ASSOCIATIONS COMPETENTES EN MATIERE DE SANTE **30**

ANNEXE 1 : DECRET N°2006-6 DU 4 JANVIER 2006 RELATIF A L'HEBERGEMENT DE DONNEES DE SANTE A CARACTERE PE RSONNEL ET MODIFIANT LE CODE DE LA SANTE PUBLIQUE (DISPOSITIONS REGLEMENTAIRES) 31

ANNEXE 2 :

- ARRETE DU 7 FEVRIER 2006 FIXANT LA COMPOSITION DU COMITE D'AGREMENT DES HEBERGEURS DE DONNES DE SANTE A CARACTERE PERSONNEL 40

- ARRETE DU 21 FEVRIER 2006 MODIFIANT L'ARRETE du 7 FEVRIER 2006 FIXANT LA COMPOSITION COMPOSITION DU COMITE D'AGREMENT DES HEBERGEURS DE DONNEES DE SANTE A CARACTERE PERSONNEL 41

- ARRETE DU 15 FEVRIER 2007 MODIFIANT LES ARRETES DU 7 FEVRIER 2006 ET DU 21 FEVRIER 2006 FIXANT LA COMPOSITION DU COMITE D'AGREMENT DES HEBERGEURS DE DONNEES DE SANTE A CARACTERE PERSONNEL 42

- ARRETE DU 19 NOVEMBRE 2009 PORTANT MODIFICATION DE L'ARRETE DU 7 FEVRIER 2006 FIXANT LA COMPOSITION DU COMITE D'AGREMENT DES HEBERGEURS DE DONNES DE SANTE A CARACTERE PERSONNEL 43

- ARRETE DU 14 JUIN 2011 FIXANT LA COMPOSITION DU COMITE D'AGREMENT DES HEBERGEURS DE DONNEES DE SANTE A CARACTERE PERSONNEL 44

ANNEXE 3 : FAQ SUR LE REFERENTIEL DE CONSTITUTION DES DOSSIERS DE DEMANDE D'AGREMENT 46

ANNEXE 4 : REPONSE EN DATE DU 10 MAI 2011 DE LA MISSION JURIDIQUE DES AFFAIRES SOCIALES, SUR L'APPLICATION DE LA PROCEDURE D'AGREMENT AUX BASES DE DONNEES DE RECHERCHES BIOMEDICALES 56

INTRODUCTION

Le Comité d'agrément des hébergeurs de données de santé à caractère personnel mis en place en février 2006 a terminé sa première période quinquennale d'activité. Ce rapport présente son fonctionnement, les avis qu'il a rendus et la doctrine progressivement dégagée de ses décisions. Ce premier bilan permet également de proposer des évolutions afin de faciliter les procédures et d'adapter les référentiels.

Les membres du Comité d'agrément ont été nommés par l'arrêté du 14 juin 2011 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel (JORF n°0140 du 18 juin 2011 page 10455 texte n° 39), les mandats initiaux ayant atteint leur terme.

TITRE 1 : L'ENCADREMENT DE L'HÉBERGEMENT DES DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL

Le recours à des tiers spécialisés dans la conservation électronique, communément appelés *« hébergeurs »*, devient progressivement la règle pour les établissements de santé, mais également pour les professionnels de santé et particulièrement les radiologues.

En outre, des industriels développent des offres d'hébergement -coffres-forts électroniques- à destination des particuliers, afin qu'ils puissent y déposer des documents divers contenant leurs données de santé dont des comptes rendus médicaux.

Pressentant ces évolutions, le législateur s'est préoccupé dès la loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé d'encadrer ces pratiques, afin de maintenir un haut niveau de sécurité, gage de la confiance des personnes concernées par les données de santé et des professionnels.

L'hébergement de données de santé à caractère personnel est une activité qui nécessite la mise en oeuvre de traitements automatisés. Il est donc soumis au respect de la loi n°78-17 du 6 janvier 1978, modifiée relative à l'informatique, aux fichiers et aux libertés et au contrôle de la Commission Nationale de l'Informatique et des Libertés (CNIL).

L'agrément ministériel constitue une garantie supplémentaire et d'une autre nature, en particulier dans les domaines où la compétence de cette institution ne peut s'exercer. Il en est ainsi, par exemple, dans le domaine éthique, où il convient d'écarter les hébergeurs susceptibles de présenter des conflits d'intérêts et dans le domaine économique et financier, où il convient d'écarter du marché des sociétés fragiles au modèle économique incertain, dont l'interruption d'activité aurait des conséquences lourdes sur la conservation des données. Pour ce qui concerne le respect des droits des patients et la sécurité des données, le législateur a donné au Comité d'agrément des compétences qui recoupent en partie celles de la CNIL, celle-ci assurant par ailleurs un contrôle sur les responsables de traitement.

A- LE CADRE JURIDIQUE ET LE PÉRIMÈTRE DE L'HÉBERGEMENT DE DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL

Les données de santé à caractère personnel sont inhérentes à la vie privée des individus. Leur caractère sensible a conduit le législateur à encadrer l'hébergement de ces données.

Le cadre juridique de l'hébergement de données de santé à caractère personnel est posé par l'article L1111-8 alinéa 1er du code de la santé publique qui dispose que «*les professionnels de santé, les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel recueillies ou produites à l'occasion d'activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet. Cet hébergement de données, quel qu'en soit le support papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée* ».

La procédure d'agrément a été précisée par le décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel sur support électronique.

Pour exemple, lorsqu'un établissement de santé disposant d'un système d'information sécurisé héberge des données de santé à caractère personnel pour le compte d'autres établissements de santé, il se trouve en position d'hébergeur de données de santé à caractère personnel et doit déposer un dossier de demande d'agrément pour l'hébergement de données de santé à caractère personnel.

Lorsqu'un établissement de santé ou un professionnel de santé conserve lui-même, par ses propres moyens, les données de santé à caractère personnel de ses patients, il n'est pas soumis à la procédure d'agrément.

La procédure d'agrément pour l'hébergement de données de santé à caractère personnel sur support papier a été précisée récemment par le décret n°2011-246 du 4 mars 2011 relatif à l'hébergement de données de santé à caractère personnel sur support papier. Cet agrément est délivré par le ministre chargé de la culture.

B- LA NOTION D'HÉBERGEMENT

La sémantique a toujours associé au terme « hébergement » deux notions : l'accueil et la protection. Cette connotation valorisante est particulièrement justifiée pour les données de santé à caractère personnel.

La nature sensible des données de santé à caractère personnel impose qu'elles soient stockées au moyen de techniques les plus performantes garantissant leur sécurité, leur confidentialité, leur intégrité, leur pérennité et leur traçabilité.

En effet, la confiance du patient du professionnel ou de l'établissement de santé qui le prend en charge ne s'étend pas implicitement aux tiers avec lesquels ces derniers travaillent. Il est donc justifié, en cas d'externalisation des données de santé à caractère personnel, c'est-à-dire

d'hébergement, que le patient soit informé des conditions dans lesquelles les informations qui le concernent seront conservées et des garanties qui y sont attachées

Le dispositif technique de l'hébergeur doit être sécurisé afin que l'accès des professionnels de santé aux données de santé à caractère personnel hébergées ne soit permis qu'aux professionnels de santé autorisés et habilités à y accéder.

La définition de l'hébergement a été éclairée par les débats autour de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, visant à transposer la directive européenne de 2000. L'hébergeur a été défini comme assurant un stockage *permanent ou du moins durable* des données et dont les fonctions vont *au-delà du seul stockage direct,* c'est-à-dire celui qui exclut tout traitement. Cette forme de dépôt est définie par le stockage de données qui seront restituées à l'identique à celui qui les a produites.

TITRE 2 : LE DÉROULEMENT DE LA PROCÉDURE D'AGRÉMENT DES HÉBERGEURS DE DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL

Le décret n°2006-6 du 4 janvier 2006 précise le déroulement de la procédure d'agrément pour l'hébergement de données de santé à caractère personnel sur support électronique.

A- LES ACTEURS DE LA PROCÉDURE D'AGRÉMENT

1) Le candidat

Le candidat à l'agrément peut être toute personne physique ou morale qui souhaite héberger des données de santé à caractère personnel.

2) La Commission nationale de l'informatique et des libertés (CNIL)

La Commission nationale de l'informatique et des libertés est chargée d'instruire les dossiers de demande d'agrément, afin d'apprécier les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données.

Elle émet un avis sur les dossiers de demande d'agrément, qu'elle transmet au Comité d'agrément.

3) Le Comité d'agrément

L'article R1111-10 du code de la santé publique issu du décret n°2006-6 du 4 janvier 2006 crée un *« Comité d'agrément »* placé auprès du ministre de la santé, chargé d'émettre un avis sur les dossiers de demande d'agrément. Cet avis est transmis au Ministre chargé de la santé.

L'arrêté du 14 juin 2011 fixe la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel (Annexe 2).

4) Le Ministre chargé de la santé

Le Ministre est chargé de délivrer l'agrément aux hébergeurs de données de santé à caractère personnel qui en ont fait la demande. Cet agrément est délivré pour 3 ans à compter de la décision.

Ses missions sont les suivantes :

- Nomination des membres du comité d'agrément et publication des arrêtés de nomination ;
- Notification des décisions d'agrément ou de refus d'agrément ;
- Communication aux candidats, le cas échéant, des motifs de refus d'agrément et des recommandations accompagnant les décisions d'agrément ;
- Publication des avis d'agrément au Bulletin officiel du Ministère de la Santé.

5) L'Agence des systèmes d'information partagés de santé (ASIP Santé)

Le Secrétaire Général du ministère chargé des affaires sociales a confié depuis mars 2009 à l'ASIP Santé, la mission d'instruire les dossiers de demande d'agrément à l'hébergement de données de santé à caractère personnel, afin d'assister le Comité d'agrément et lui permettre de traiter efficacement dans des délais raisonnables les dossiers.

Pour mener à bien cette mission, un comité d'instruction interne à l'ASIP Santé a été mis en place. Ce Comité d'instruction pré-instruit les dossiers de demande d'agrément sous trois volets :

- un volet éthique et juridique, correspondant à l'examen des garanties d'ordre éthique et déontologique en relation avec la pratique et les finalités médicales de l'hébergement de données de santé à caractère personnel et le respect des droits du patient ;
- un volet sécurité et technique, présentant les résultats de l'analyse du dossier sur les garanties apportées en terme de politique de sécurité des systèmes d'information et de confidentialité des données de santé, en considérant les aspects techniques mais également organisationnels ;
- un volet économique et financier, analysant le modèle économique et la structure financière du candidat.

L'Agence des systèmes d'information partagés de santé (ASIP Santé) est également en charge depuis le 1er mars 2010 du secrétariat du comité d'agrément. Cette mission lui a été confiée par la Délégation à la stratégie des systèmes d'information de santé.

A ce titre, l'ASIP Santé est responsable de la retranscription par écrit des avis du Comité d'agrément et de l'envoi de ces avis au Ministre chargé de la santé.

Le secrétariat du comité d'agrément rédige également les courriers envoyés aux candidats (lettre de refus motivée, proposition de décision d'agrément…).

B- LE DÉROULEMENT DE LA PROCÉDURE

L'article R1111-10 du code de la santé publique issu du décret n°2006-6 du 4 janvier 2006 décrit le processus global de traitement d'une demande d'agrément.

1) La réception du dossier de demande d'agrément

Le candidat envoie, en recommandé avec accusé de réception, son dossier de demande d'agrément au format électronique sur CD-ROM ou DVD-ROM, ainsi que deux exemplaires sous format papier au secrétariat du comité d'agrément.

Dès réception, le candidat reçoit un courrier du secrétariat du comité d'agrément lui indiquant la bonne réception de son dossier.

Si le dossier est incomplet, en ce sens qu'il manque un des formulaires auxquels le candidat doit répondre, un courrier lui est adressé afin qu'il complète sa demande.

Le dossier de demande d'agrément reçu est transmis le jour même à la Commission nationale de l'informatique et des libertés.

2) L'instruction du dossier par l'ASIP Santé et la CNIL

a) Dès réception des dossiers et en fonction de leur ordre d'arrivée, les chargés d'analyse désignés au sein de l'ASIP Santé instruisent les dossiers de demande d'agrément sous trois angles : éthique et juridique, sécurité et technique et économique et financier.

Des rapports d'instruction sont rédigés et présentés lors du comité d'instruction interne, qui permet aux chargés d'analyse d'échanger leurs points de vue sur le dossier et de dégager les points positifs et les points sensibles du dossier. Les rapports d'instruction doivent être validés par le responsable de ce comité.

C'est alors que les chargés d'analyse rencontrent un des membres du Comité d'agrément *« rapporteur »* du dossier pour lui présenter le dossier.

b) Parallèlement, la CNIL instruit également le dossier de demande d'agrément dans un délai de deux mois, renouvelable une fois, sur décision motivée de son président. La CNIL émet un avis qu'elle transmet au Comité d'agrément.

c) L'avis du comité d'agrément

Dans un délai d'un mois suivant la réception de l'avis de la CNIL (délai renouvelable une fois), le comité d'agrément se réunit. Chaque *« rapporteur »* présente le dossier pour lequel il a été désigné aux autres membres du comité d'agrément.

Les chargés d'analyse et le responsable du comité d'instruction interne de l'ASIP santé, ainsi que des agents de la CNIL assistent aux séances du Comité d'agrément afin d'apporter, si nécessaire, des précisions supplémentaires aux membres du comité d'agrément.

Le comité d'agrément se prononce sur tous les aspects du dossier, en particulier sur les garanties d'ordre éthique, déontologique, technique, financier et économique qu'offre le candidat, et rend un avis.

Cet avis est transmis par le secrétariat du comité d'agrément au Ministre chargé de la santé.

d) La décision du Ministre chargé de la santé

Le Ministre chargé de la santé dispose d'un délai de deux mois suivant la réception de l'avis du Comité d'agrément pour prendre sa décision. A l'issu de ce délai, son silence vaut décision de rejet.

Le candidat reçoit un courrier lui notifiant la décision d'agrément ou le refus d'agrément. Ce courrier peut être accompagné de recommandations.

Les décisions d'agrément sont publiées au Bulletin officiel du ministère de la santé.

L'agrément est délivré pour une durée de trois ans. Toute demande de renouvellement de l'agrément doit être déposée au plus tard six mois avant le terme de la période d'agrément.

TITRE 3 : L'ACTIVITÉ DU COMITÉ D'AGRÉMENT

A- UN PREMIER BILAN GLOBALEMENT POSITIF

✓ L'élaboration d'un référentiel

Le Comité d'agrément est exclusivement compétent pour les traitements :

- contenant des données de santé à caractère personnel ;
- externalisés, c'est à dire non conservés par le producteur des données ;
- présentés sous format électronique.

Il convient de préciser que le CAH a été réuni en 2006 à l'occasion des demandes d'agréments présentées par les 6 consortiums ayant soumissionné pour héberger le dossier médical personnel. Le 22 mai 2006, le Ministre a prononcé 6 décisions d'agrément. L'activité du Comité d'agrément a ensuite été suspendue pendant une période de 2 ans à compter du 2 février 2007[1].

Les travaux d'élaboration du référentiel de constitution des dossiers de demandes d'agrément des hébergeurs de donnés de santé ont été relancés fin 2008 à la demande de l'ex-Mission pour l'informatisation du secteur santé social (ex MISS, devenue Délégation à la Stratégie des Systèmes d'Information de Santé) placée auprès du ministère en charge de la santé.

Le Groupement d'intérêt public du Dossier Médical Personnel, devenu Groupement d'intérêt public Agence des Systèmes d'Information partagés de Santé (ASIP Santé), dont la convention constitutive a été approuvée par arrêté du 8 septembre 2009, s'est alors vu confier l'élaboration des référentiels de constitution des dossiers de candidature à l'agrément à l'hébergement de données de santé à caractère personnel, ainsi que la pré-instruction des dossiers d'instruction au profit du Comité d'agrément des hébergeurs.

Ces travaux ont été réalisés en concertation avec les opérateurs, les industriels et les maîtrises d'ouvrage régionales du secteur de la santé. Les industriels étaient présents à travers leurs organisations représentatives : LESISS, SNITEM, SYNTEC …

Les participants se sont accordés pour considérer qu'un candidat à l'agrément doit démontrer aux pouvoirs publics qu'il mobilise des moyens conséquents et adaptés permettant de satisfaire à la sécurité et à la confidentialité des données de santé à caractère personnel. L'objectif est clairement d'élever le niveau de sécurité des bases de données de santé à caractère personnel. Il est également de traduire de façon concrète les exigences d'un texte réglementaire long et compliqué.

Le consensus obtenu avec les acteurs du secteur a débouché, d'une part, sur l'obligation de réaliser et d'argumenter une analyse de risques sécurité du système d'information (SSI) sur le périmètre de la prestation d'hébergement et, d'autre part, sur l'obligation de démontrer la couverture de l'ensemble des exigences de sécurité définies dans le décret.

Cinq réunions ont permis d'octobre 2008 à février 2009 de définir les conditions du traitement d'une demande d'agrément qui se fonde sur le dépôt d'un dossier conforme au référentiel de constitution des dossiers.

---

[1] Suspension de la procédure d'agrément par l'article 25 IV de la loi n°2007-127 du 30 janvier 2007 *:« Sauf lorsqu'elle s'applique à des demandes d'agrément portant sur l'hébergement des dossiers médicaux personnels prévus à l'article L.161-36-1 du code de la sécurité sociale, la procédure d'agrément prévue à l'article L.1111-8 du code de la santé publique est suspendue pendant une période de deux ans à compter de la publication de la présente loi. Pendant le délai de deux ans prévu à l'alinéa précédent, toute personne peut exercer l'activité d'hébergement de données de santé à caractère personnel, autres que celles constituant le dossier médical personnel prévu à l'article L.161-36-1 du code de la sécurité sociale, à condition de satisfaire aux dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La poursuite de cette activité au-delà de la période transitoire est subordonnée au dépôt d'une demande d'agrément avant l'expiration de ladite période. L'activité d'hébergement peut alors être poursuivie jusqu'à ce qu'il soit statué sur cette demande.* »

La mise en place de ce référentiel assure aux candidats un traitement équitable et efficace de leurs candidatures car il normalise une formalisation stricte du contenu du dossier de demande d'agrément.

- ✓ **Quelques chiffres**

Au titre de cette première période quinquennale de fonctionnement du Comité d'agrément, le présent rapport s'appuie sur les dossiers présentés en séance du Comité d'agrément depuis le 2 février 2009, soit 30 dossiers.

21 organismes ont été agréés par le Ministre en charge de la santé en qualité d'hébergeur de données de santé à caractère personnel et 9 candidats n'ont pas obtenu l'agrément[1].

A ce jour (juillet 2011), 66 dossiers conformes ont été déposés et 11 rapports d'auto-évaluation ont été envoyés par les hébergeurs agréés.

Ces chiffres attestent de la montée en charge d'une procédure qui devient désormais une étape essentielle pour les organismes qui proposent un service d'hébergement de données de santé à caractère personnel. Le temps de la procédure reste long (entre 5 à 8 mois) mais se positionner comme candidat à l'hébergement est aujourd'hui une condition posée par les professionnels de santé, les établissements de santé et les patients eux-mêmes pour confier à des tiers la conservation de leurs données de santé.

Une foire aux questions a été construite et enrichie au fil des interrogations remontées par les candidats potentiels à l'agrément, les candidats ayant déposé un dossier et des débats du comité d'agrément des hébergeurs qui se prononce sur les dossiers de candidature. Elle est accessible sur le site de l'ASIP Santé et comporte une vingtaine de questions (Annexe 3).

B- LA QUESTION DE LA RECEVABILITÉ DES DEMANDES D'AGRÉMENT : ÉLÉMENT CLÉ DE LA PROCÉDURE

Dans le cadre de l'exercice de sa mission, le Comité s'est interrogé sur la recevabilité des demandes. En effet, certaines difficultés sont apparues.

La loi n°2002-303 du 4 mars 2002 précitée a créé un statut *« d'hébergeur agréé ».* Cependant, les différentes activités exercées par un organisme candidat à l'agrément hébergeur ne nécessitent pas toutes un agrément.

Il n'est pas paru possible de proposer au Ministre en charge de la santé un agrément général. Les dossiers présentés par les candidats doivent clairement identifier le type de prestation d'hébergement de données de santé à caractère personnel pour lequel est demandé l'agrément.

[1] Chiffres arrêtés le 28 juin 2011

Cette offre de service doit être désignée de façon à être visible et détachable des autres activités de l'hébergeur.

Ainsi, l'agrément est délivré pour un type de prestation et ne porte pas sur l'ensemble des prestations proposées par le candidat.

L'organisme peut donc être agréé autant de fois que de prestations différentes qu'il propose.

Par exemple, un organisme propose une prestation d'hébergement de PACS et une autre prestation de conservation de dossiers médicaux à destination de professionnels de santé : ce sont deux prestations distinctes qui nécessitent chacune un agrément.

Le périmètre de l'hébergement de données de santé à caractère personnel a été défini par le législateur à l'article L1111-8 du code de la santé publique. Est considérée comme hébergeur, toute personne physique ou morale qui héberge des données de santé à caractère personnel produites par un tiers à l'occasion d'activités de prévention, de diagnostic ou de soins.

Au cours de ses travaux, le Comité d'agrément a ainsi été saisi de demandes d'agrément pour lesquelles il s'est interrogé sur leur recevabilité.

- ✓ **L'exemple des *« Contract Research Organisation »* (CRO) ou sociétés de recherche sous contrat en est une illustration :**

Ces sociétés ont pour mission, sous l'autorité du promoteur d'une recherche biomédicale, de gérer la collecte, la conservation et l'exploitation des données recueillies dans le cadre de la recherche auprès des investigateurs.

Ces sociétés peuvent-elles être considérées comme hébergeurs des données relatives à l'état de santé des patients se prêtant à la recherche et conservées exclusivement à cette fin.

Les données collectées dans ce cadre sont en général indirectement nominatives, le patient étant identifié par des initiales et/ou un numéro, mais elles demeurent des données à caractère personnel.

Le Comité d'agrément a débattu de cette question, afin de savoir si les CRO devaient déposer un dossier de demande d'agrément pour l'hébergement de données de santé à caractère personnel recueillies à l'occasion de recherche dans le domaine de la santé.

Les avis ont été divergents au sein du Comité. Selon certains membres du comité d'agrément, dans la mesure où les données sont indirectement nominatives et que la table de correspondance est conservée par le médecin investigateur de la recherche, les risques pour la confidentialité des données sont très limités et l'agrément ne serait pas nécessaire. En outre, ces données pour la plupart recueillies à l'occasion d'activités de soins sont déjà soumises à des mesures de protection spécifiques.

Le code de la santé publique encadre en effet précisément la conduite de ces études (articles L1121-1 et suivants) et la loi Informatique et Libertés a défini les conditions de leur autorisation dans le chapitre IX relatif aux traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé. La CNIL a, en outre, en concertation avec les milieux de la recherche, défini

les caractéristiques des traitements propres à ces recherches biomédicales dans une méthodologie de référence (Méthodologie de référence MR-001 pour les traitements de données personnelles opérées dans le cadre de recherches biomédicales – octobre 2010). Aussi, selon ces membres, soumettre les bases de données de santé à caractère personnel créées dans le cadre d'une recherche dans le domaine de la santé à l'agrément prévu par l'article L 1111-8 du code de la santé publique, alourdirait les démarches déjà très lourdes des acteurs de la recherche.

Pour d'autres membres du Comité d'agrément, l'article L1111-8 du code de la santé publique s'applique aux CRO, en raison de la conservation de données de santé à caractère personnel par un tiers qui n'est pas le producteur des données. A cet égard, il ne serait pas justifié d'exonérer ces activités d'hébergement de l'agrément prévu par la loi, la personne dont les données sont ainsi conservées devant pouvoir bénéficier des mêmes garanties que les autres.

Face à ces divergences de position, la Mission Juridique du conseil d'Etat auprès du Ministère en charge de la santé a été saisie. Dans sa réponse du 10 mai 2011, la Mission juridique a d'abord insisté sur la nécessité d'assurer la sécurité des données de santé à caractère personnel en raison de leur sensibilité :

> « *Ces données font partie des catégories particulières dont la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel prévoit qu'elles ne peuvent être traitées à moins que le droit interne ne prévoie des garanties appropriées* ».

Se fondant sur la protection assurée en droit interne par la loi du 6 janvier 1978 informatique et libertés, la mission juridique a conclu dans les termes suivants que les bases de données de santé constituées à l'occasion de recherches biomédicales n'étaient pas soumises à la procédure d'agrément prévu à l'article L1111-8 du code de la santé publique et précisée par le décret 2006-6 du 4 janvier 2006 :

> *« En application de l'article 53 de la loi du 6 janvier 1978 informatique et libertés, les traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé sont soumis aux dispositions de cette loi, à l'exception des articles 23 à 26, 32 et 38. […]*
>
> *Nous avons donc bien deux régimes exclusifs l'un de l'autre, celui de l'hébergement des données de santé au sens de l'article L 1111-8 et celui du traitement des données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, sur le fondement de l'article L 1121-1 et de la loi du 6 janvier 1978.*
>
> *Les organismes qui veulent conserver des données de santé à des fins de recherche n'ont pas dans l'état des textes à recueillir un agrément sur la base de l'article L 1111-8 qui ne concerne que ceux répondant à la définition donnée par cet article. »*

La position complète de la Mission juridique est jointe en annexe du présent rapport (Annexe 8).

- ✓ **<u>Les opérateurs de programme d'éducation thérapeutique ont également présenté des dossiers au comité d'agrément, soulevant des questions de recevabilité de même ordre :</u>**

Aux termes de l'article L 1161-5 du code de la santé publique précisé par deux décrets et deux arrêtés de 2010[2], les programmes sont conduits par un opérateur, choisi et conventionné à cet effet par l'entreprise exploitant le médicament.

L'opérateur est choisi en fonction des garanties d'indépendance qu'il présente, de ses compétences et des moyens humains et matériels dont il dispose pour exécuter les tâches qui relèvent de la mise en œuvre du programme d'apprentissage.

Le CAH a considéré que l'activité de ces opérateurs dans la collecte des données relevait de l'encadrement prévue par le décret du 4 janvier 2006.

Une société a ainsi été agréée pour l'hébergement de données de santé à caractère personnel dans le cadre de programmes d'éducation thérapeutique (société H2AD).

TITRE 4 : ARTICULATION DES EXPERTISES DU COMITÉ D'AGRÉMENT ET DE LA CNIL

A- LA CNIL DANS LA PROCÉDURE D'AGRÉMENT

La CNIL intervient également dans la procédure d'agrément par la transmission d'un avis sur les dossiers d'agrément au Comité d'agrément.

Aussi, le Comité d'agrément a estimé important d'assurer une concertation étroite avec la CNIL, afin de fluidifier les procédures, tout en conservant la souveraineté de son appréciation sur les dossiers de demande d'agrément.

Là où les compétences et les champs d'investigation de ces deux acteurs sont communs, cette concertation permet de proposer une doctrine homogène et lisible.

Enfin, il est essentiel pour assurer les meilleures garanties aux patients et acteurs de la chaîne de soins que l'ensemble des étapes du processus d'hébergement soient contrôlées.

---

2 Les textes :

- ✓ Décret n° 2010-906 du 2 août 2010 relatif aux compétences requises pour dispenser l'éducation thérapeutique du patient
- ✓ Arrêté du 2 août 2010 relatif aux compétences requises pour dispenser l'éducation thérapeutique du patient
- ✓ Décret n° 2010-904 du 2 août 2010 relatif aux conditions d'autorisation des programmes d'éducation thérapeutique du patient
- ✓ Arrêté du 2 août 2010 relatif au cahier des charges des programmes d'éducation thérapeutique du patient et à la composition du dossier de demande de leur autorisation

Ainsi, la CNIL est chargée au titre de la Loi Informatique et Libertés de s'assurer du respect par le responsable du traitement des principes de la protection des données personnelles. A ce titre, elle connaît les conditions du respect des droits de la personne par le responsable du traitement avant qu'il ne recoure à l'hébergement.

Compte tenu des rôles spécifiques des deux instances, une vision globale du dossier est indispensable. Cette concertation doit se poursuivre au cours de la prochaine période quinquennale.

Selon les termes du décret n°2006-6 du 4 janvier 2006, « *le Comité d'agrément se prononce après avis de la CNIL, qui doit apprécier les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données »*.

Il est apparu nécessaire d'organiser les procédures d'examen des dossiers des candidats de façon à articuler et respecter les délais de procédures fixés par le décret n°2006-6 du 4 janvier 2006 ; tant concernant l'avis de la CNIL (deux mois renouvelables), que du CAH (un mois renouvelable). En effet, les dossiers d'agrément sont examinés de façon systématique par la séance plénière de la CNIL, ce qui contraint les calendriers.

Aux termes d'une concertation, l'ASIP Santé qui assure le secrétariat du Comité d'agrément et la pré-instruction des dossiers de demande d'agrément pour le compte du Comité d'agrément et dont elle fait également bénéficier la CNIL, a mis en place un cahier des charges type que doivent renseigner les candidats. Cela permet de raccourcir au mieux les délais courant après le dépôt de candidature.

A compter de la remise du dossier par le candidat et jusqu'à la séance du Comité d'agrément, les deux procédures se déroulent de manière indépendante sans préjudice d'un éventuel échange d'informations pour une meilleure efficacité. L'avis de la CNIL est transmis au Comité d'agrément avant la séance.

LA CNIL ET LES CONTRÔLES PAR FRÉDÉRIQUE LESAULNIER

Commission Nationale de l'Informatique et des Libertés
Direction des affaires juridiques, internationales et de l'expertise
Juriste en charge du secteur de la santé

Les hébergeurs de données de santé placés *« sous contrôle »*

La numérisation des données de santé de chaque citoyen et l'entrée d'internet dans l'univers médical sont porteuses de promesses majeures pour l'individu et pour la collectivité. Elles sont également porteuses de menaces nouvelles pour la protection des données personnelles, compte tenu des risques de divulgation, d'utilisation détournée et de déformation des données liés à l'utilisation d'Internet. Il est évident qu'avec la multiplication des transmissions de données médicales et l'accroissement du nombre d'acteurs susceptibles d'accéder aux réseaux informatiques, le déploiement de solutions de sécurité effectives et de haut niveau est aujourd'hui une priorité renforcée. Les données de santé sont des données sensibles, susceptibles de révéler l'intimité de la vie privée. A ce titre, le droit leur reconnaît un statut particulier et impose le respect de règles ayant pour objet de garantir leur confidentialité, auquel la CNIL veille depuis près de trente ans.

L'externalisation des données de santé auprès d'un organisme spécialisé, distinct du professionnel ou de l'établissement de santé qui soigne le malade, a ainsi été placée sous contrôle. La loi n° 2002-303 du 4 mars 2002 relative aux droits des malades, complétée par le décret n°2006-6 du 4 janvier 2006, a organisé un encadrement juridique et technique de l'hébergement des données personnelles de santé que la CNIL avait appelé de ses vœux.

La CNIL, qui participe à la procédure d'agrément des hébergeurs et à la réflexion sur l'évolution de cette procédure, a également décidé d'inscrire les hébergeurs de données de santé à caractère personnel à l'ordre du jour de son programme annuel des contrôles. Le but recherché est d'amener les acteurs de l'hébergement au plus haut niveau de sécurité afin d'offrir un espace de confiance aux patients et aux professionnels.

Un ordre public propre à garantir la sécurité des données de santé est ainsi en cours de construction auquel la CNIL entend participer activement en concertation avec l'ensemble des acteurs concernés.

B- L'HOMOGÉNÉITÉ DE LA DOCTRINE DU COMITÉ D'AGRÉMENT ET DE LA CNIL

Le respect des droits des patients est un point essentiel de l'analyse des dossiers. Dans la plupart des dossiers examinés, ces obligations sont reportées contractuellement sur le client de l'hébergeur, généralement établissement de santé ou professionnel de santé.

- ✓ **Le respect de la confidentialité des traitements contenant des données de santé à caractère personnel est un élément important.**

Les conditions d'accès aux informations des professionnels de santé et, le cas échéant, des patients doivent reposer sur des moyens permettant une identification et une authentification forte et conformes aux dispositions de l'article L1111-8 alinéa 4 du code de la santé publique qui renvoie à l'article L1110-4 alinéa 4 du même code, ce dernier faisant référence à l'utilisation d'une carte CPS (Carte de Professionnel de Santé) ou d'un dispositif équivalent.

Le Comité d'agrément et la CNIL, conscients des évolutions actuelles relatives à la CPS et de l'état de diffusion de cette carte, adoptent une position pragmatique, afin de permettre le fonctionnement des établissements de santé, tout en assurant la sécurité des échanges de données.

- ✓ **La confidentialité impose un contrôle strict des accès du personnel de l'hébergeur.**

Ce point fait débat au sein du CAH et a été directement rapproché de celui relatif à la nécessité ou pas de recourir au chiffrement des bases de données. Les partisans d'un chiffrement obligatoire des bases de données contenant des données de santé à caractère personnel s'opposent à ceux pour lesquels il ne constitue pas la solution unique permettant d'assurer la sécurité des données. Une politique de sécurité fondée sur une bonne expertise préalable des risques et associant une série de mesures permettant d'assurer la légitimité des accès (habilitation, traçabilité,…) est de toute manière indispensable.

Lorsqu'un chiffrement est mis en place, il doit toujours être possible d'accéder à la donnée de santé. Il convient donc de s'assurer de la réversibilité de l'encodage au moyen du maintien opérationnel des clés de chiffrement quelle que soit l'évolution technologique. La CNIL a entamé une réflexion sur l'obligation de chiffrement des bases et des transferts. Cette réflexion sera mise en perspective avec les travaux de l'ASIP Santé et discutée prochainement au sein du Comité d'agrément.

Aujourd'hui, le chiffrement des données de santé à caractère personnel hébergées n'est pas une exigence du décret n°2006-6 du 4 janvier 2006.

Enfin, lorsque le stockage des données est assuré physiquement dans un Etat membre de l'Union européenne ou aux USA, le CAH impose les mêmes exigences que la CNIL.

- ✓ **Continuité du service et pérennité.**

La sécurité impose de protéger les données de telle sorte qu'elles ne puissent être ni altérées, ni détruites. Les exigences de sécurité concernent également la continuité du service, sur le long terme, en cas d'incident technique. L'exigence de pérennité vise à maintenir de façon stable le stockage des données. Cette exigence est remplie lorsqu'existe un deuxième site de stockage suffisamment éloigné, afin qu'il soit épargné lors d'une éventuelle catastrophe industrielle ou naturelle. Cette exigence peut être également satisfaite lorsque des sauvegardes régulières sur un support physique sont faites et les supports transportés dans un lieu de stockage à l'abri d'un sinistre qui frapperait le site principal. Les qualités du support physique susceptibles d'altérer les données doivent donc être précisées.

Concernant les niveaux de disponibilité et de performance et la continuité du service en cas d'incident, le candidat doit fournir des renseignements sur la durée maximum de perte de données en cas de sinistre avant que le service soit rétabli. Ce paramètre dépend également des caractéristiques du système informatique du client et du logiciel utilisé.

TITRE 5 : LA DOCTRINE PROPRE AU COMITÉ D'AGRÉMENT

Cette doctrine est exprimée dans ce rapport mais certains points sont développés dans la Foire aux questions consultable sur le site esante.gouv.fr et annexée au présent rapport dans son dernier état (Annexe 3).

A- LES CARACTÉRISTIQUES DU DOSSIER DE DEMANDE D'AGRÉMENT

1) Le candidat

Le candidat doit être clairement identifié. L'activité principale du candidat à l'agrément doit être décrite.

Le candidat doit mentionner dans son dossier les personnes (son personnel ou personnel des sous-traitants) qui peuvent avoir accès aux données dans le cadre de leurs missions, même lorsque les données sont chiffrées.

Le Comité a constaté dans plusieurs dossiers des carences sur les garanties à fournir pour les personnels employés: administrateurs et techniciens.

La mise en place de mots de passe individuels strictement personnels (et non collectifs) est impérative et doit être associée à une politique de gestion des mots de passe à préciser (robustesse, fréquence de renouvellement).

2) Le client

Le candidat doit clairement identifier les profils de clients à qui il souhaite proposer la prestation objet de la demande d'agrément. Cela est indispensable pour la bonne compréhension du dossier.

3) La personne concernée par les données hébergées (le patient)

Le respect des droits des patients doit être garanti soit par le candidat lui-même, soit par le client par un report contractuel strictement défini.

4) Le médecin de l'hébergeur

Le décret n°2006-6 du 4 janvier 2006 (article R 1111-9 du code de la santé publique) impose au candidat de désigner un médecin et de préciser les liens contractuels avec ce dernier. Ce « médecin de l'hébergeur » joue un rôle nouveau créé par le décret précité.

Il est le gardien du respect du secret professionnel dans le cadre du contrat qui le lie à l'hébergeur. Il agit dans le cadre des obligations précisées dans le contrat conclu avec l'hébergeur. Aussi, le contrat conclu entre le candidat et le médecin de l'hébergeur doit être joint au dossier et transmis au Conseil départemental de l'Ordre dont ce dernier dépend, comme doit l'être tout contrat de droit privé conclu par un médecin. Lorsque le médecin de l'hébergeur est déjà salarié du candidat à l'agrément, il est nécessaire de prévoir un avenant à son contrat de travail pour insérer ses missions de médecin de l'hébergeur. Le contrat initial ainsi que l'avenant doivent être joints au dossier et envoyés au Conseil départemental de l'Ordre des médecins.

L'ASIP Santé a travaillé en collaboration avec le Conseil national de l'ordre des médecins (CNOM) et la CNIL pour définir les missions du médecin de l'hébergeur.

Le CNOM a publié sur son site un modèle de contrat type du médecin de l'hébergeur établi à partir de clauses types élaborées par l'ASIP Santé. Ce modèle de contrat permet d'offrir un texte correspondant au mieux aux exigences professionnelles.

Lorsque le médecin de l'hébergeur est salarié du candidat à l'agrément, la fonction exercée doit l'être conformément à l'article 95 du code de déontologie médicale (article R4127-95 du code de la santé publique) et le placer dans une situation d'indépendance sur le plan déontologique vis-à-vis de son employeur. Pour le Comité, la lecture qui doit être faite de cette clause interdit au médecin de l'hébergeur d'exercer des fonctions de direction associées à une rémunération proportionnelle au chiffre d'affaires.

Mais le médecin de l'hébergeur, s'il doit exercer ses missions en toute indépendance dans les conditions sus-décrites, doit concomitamment tenir compte du nécessaire respect des obligations qui résultent du contrat conclu avec l'hébergeur.

Ainsi, le médecin de l'hébergeur ne saurait, sans engager la responsabilité de l'hébergeur vis-à-vis du responsable du traitement telle que définie dans le contrat initial d'hébergement - et sur le fondement duquel l'hébergeur a reçu son agrément -, refuser d'exécuter une action qui fait partie de la prestation d'hébergement.

Autrement dit, les missions du médecin hébergeur s'exercent dans le cadre de l'organisation prévue dans le contrat qui lie l'hébergeur au responsable du traitement et dans le cadre de l'exécution de son contrat de travail. Il ne bénéficie pas d'un statut particulier mais exerce une mission particulière avec une subordination hiérarchique et une indépendance déontologique.

Quelques précisions sur les missions du médecin de l'hébergeur :

Le médecin de l'hébergeur veille à la confidentialité des données de santé à caractère personnel hébergées et au respect des conditions d'accès à celles-ci telles que définies dans la (les) prestation(s) d'hébergement. A cette fin, il peut faire toute recommandation utile.

Il veille, en accord avec la personne physique ou morale à l'origine de l'hébergement et le correspondant Informatique et Libertés s'il existe au sein de la structure d'hébergement, au respect des droits de la personne dont les données de santé à caractère personnel sont hébergées, en particulier en s'assurant de l'exercice effectif des droits ouverts au titre de la loi du 6 janvier 1978 modifiée relative à l'Informatique, aux fichiers et aux libertés. A cet effet, il peut élaborer des règles de bonnes pratiques.

Il peut être saisi de toute demande du responsable du traitement ou de toute personne habilitée visant à procéder aux vérifications de cohérence en cas de soupçons de collision ou de doublon au sein des dossiers médicaux.

Pour l'exercice de ses missions, le médecin de l'hébergeur accède aux données de santé à caractère personnel hébergées. Ces missions s'exercent sans préjudice de celles qui peuvent être exercées directement par le professionnel de santé saisi par le patient et dûment autorisé à cet effet.

Ces missions s'exercent sous réserve de l'organisation prévue dans le contrat de prestation qui lie l'hébergeur au responsable du traitement à l'exception des missions qui imposent l'accès aux données de santé à caractère personnel qui seules peuvent être satisfaites par le médecin de l'hébergeur, ou du moins en sa présence.

Au sens de la loi Informatique et libertés, l'hébergeur reste un prestataire qui agit au nom et pour le compte de son client, le responsable de traitement. Ce dernier est seul responsable de la gestion du risque liée aux traitements et peut requérir son prestataire hébergeur, dans le cadre de son contrat, pour accéder à des données de santé dès lors qu'il l'estime nécessaire pour la bonne gestion des données dont il assure le traitement. Le médecin de l'hébergeur évaluera, en fonction des données auxquelles il accède, la conduite à tenir dans l'intérêt du patient concerné et rendra compte de son action à son employeur et au client sans rupture de confidentialité. Le médecin hébergeur agit pour le compte du responsable de traitement, sous l'autorité de l'hébergeur.

Il convient de souligner que le modèle de contrat ne prévoit pas une obligation d'alerte auprès d'organises de régulation extérieurs (particulièrement le Conseil de l'Ordre), en cas de découverte d'un manquement aux règles de confidentialité. Une clause analogue à celles existant dans les contrats des commissaires aux comptes en cas de découverte d'irrégularités financières aurait constitué une garantie supplémentaire.

Afin de parfaire sa doctrine, le comité d'agrément nouvellement constitué par arrêté du 14 juin 2011 a décidé d'auditionner des médecins d'hébergeurs.

B- LE CONTRAT D'HÉBERGEMENT

- ✓ **Conformément à l'article R 1111-12 5° du code de la santé publique, la prestation d'hébergement proposée doit faire l'objet d'un contrat conclu entre l'hébergeur et son client.**

Le contenu de ce contrat est précisé à l'article R 1111-13 du code de la santé publique.

Selon le type de prestation proposée, l'hébergeur contracte soit avec un professionnel de santé, un établissement de santé ou un éditeur de logiciel santé, soit directement avec la personne concernée par les données de santé hébergées (cas plus rare).

On constate que dans l'immense majorité des cas, l'hébergeur n'entretient aucune relation directe avec le patient (personne concernée par les données de santé hébergées), mais plutôt avec les établissements de santé ou les professionnels de santé qui le prennent en charge.

Aussi, il est apparu essentiel de vérifier le respect par l'hébergeur de son devoir de conseil vis-à-vis de ses clients en relation directe avec les patients.

Compte tenu des liens indirects entre l'hébergeur et le patient, l'hébergeur peut ne pas être en mesure de répondre personnellement à certaines exigences du décret n°2006-6 du 4 janvier 2006. Le Comité d'agrément a donc jugé essentiel que les contrats d'hébergement détaillent précisément la répartition des responsabilités entre l'hébergeur et son client.

Lorsque l'hébergeur reporte par des clauses contractuelles claires et précises certaines exigences du décret, il doit user de son devoir de conseil.

Ainsi, lorsque le candidat reporte sur son client le recueil du consentement exprès de la personne concernée à l'hébergement de ses données de santé, les modalités de recueil du consentement doivent être décrites. Un formulaire de recueil du consentement doit être formalisé et joint au dossier.

Les modalités d'exercice par le patient de ses droits d'accès, de rectification ou d'effacement de ses données de santé doivent être décrites.

L'hébergeur doit également conseiller et informer ses clients sur l'application de la loi *« informatique et libertés ».*

- ✓ **Lorsque les modalités d'accès des professionnels de santé et la gestion de la politique d'habilitation des professionnels de santé sont reportées sur le client, l'hébergeur doit clairement mentionner ce report dans le contrat d'hébergement et doit user de son devoir de conseil quant à l'utilisation de la carte CPS ou de dispositifs équivalents.**

Le Comité d'agrément estime que l'hébergeur est investi d'une obligation de conseil renforcée vis-à-vis de son client. Le non respect des obligations légales par le client peut entraîner la rupture du contrat le liant à l'hébergeur et le non respect par l'hébergeur de ses obligations de prestataire telles que prévues au contrat peut également conduire le client à mettre un terme à l'hébergement.

Les contrats doivent préciser le niveau de disponibilité du service réellement garanti au client et la prise en compte de la continuité de ce service. Les exigences seront d'autant plus fortes lorsque la prestation est délivrée à des professionnels de santé n'ayant pas nécessairement une culture informatique aussi développée que celle du service informatique d'un hôpital.

C- LE CONTRAT AVEC LES SOUS-TRAITANTS

La procédure d'agrément est exigée pour le seul hébergeur, toutefois, ce dernier doit souvent faire appel à des tiers pour la fourniture de la prestation d'hébergement proposée à ses clients. Par exemple pour le stockage physique des données (salle claire).

Ces tiers sont donc des sous-traitants du candidat. Les différents sous traitants de l'hébergeur doivent être présentés, localisés et leurs fonctions précisées dans la chaîne d'hébergement.

Si des personnels du sous-traitant peuvent avoir accès aux données de santé hébergées ils doivent être identifiés, dans les mêmes conditions que pour le personnel du candidat.

Le contrat de sous-traitance doit être joint au dossier.

Le Comité juge ainsi nécessaire d'étudier précisément les conditions d'activité du sous-traitant, la nature de ses systèmes de sécurité et les exigences imposées à son personnel. Celles-ci doivent être de même nature que celles imposées au personnel de l'hébergeur. Le contrat de sous-traitance doit rappeler la sensibilité particulière des données de santé, d'autant plus que de nombreux sous-traitants ont des activités généralistes (données financières, etc).

D- BILAN ÉCONOMIQUE ET FINANCIER

L'alinéa 6 de l'article R 1111-12 du code de la santé publique impose la production de comptes prévisionnels et de bilans de l'activité d'hébergement.

Le comité s'est trouvé face à deux cas de figure ne lui permettant pas d'exercer efficacement sa mission :

- l'hébergeur est la filiale d'un groupe industriel français, européen ou mondial coté sur des marchés internationaux. La consultation des bilans se résume à un exercice formel dénué de toutes possibilités sérieuses de vérification. Même déficitaire, l'activité d'une filiale peut être maintenue pour des raisons industrielles.

  Dans ce cas, il paraîtrait judicieux de demander un document émanant de la société mère et l'engageant sur le maintien de l'activité d'hébergement.

- l'hébergeur est une coopérative ou un syndicat inter-hospitalier. Le bilan financier est très généralement déficitaire, ce qui n'interdit en rien le maintien de l'activité d'hébergement. Indispensable à l'activité du groupement hospitalier. Le maintien, le transfert d'activité peuvent dépendre alors de considérations politiques et administratives locales ou régionales.

  Dans ce cas, il pourrait être envisagé de demander un document auprès de l'Agence Régionale de Santé afin qu'elle précise la politique qu'elle entend mener en termes d'hébergement de santé et les structures dont l'existence va subsister après restructuration.

Lorsque l'examen du dossier ne permettait pas d'apprécier la rentabilité future, le Comité s'est attaché à vérifier que les conditions de restitution des données en cas d'arrêt d'activité étaient précisément détaillées.

E- RECOMMANDATIONS PERMETTANT AUX CANDIDATS DE MIEUX PRÉSENTER LES ASPECTS SÉCURITÉ ET TECHNIQUE

Il serait pertinent que les candidats présentent leur service d'un point de vue fonctionnel et technique global afin de fournir une vision générale du service proposé et des moyens mis en œuvre. Les éléments précis d'architecture et de sécurité devraient préférentiellement être décrits dans le formulaire *"P6-Description des dispositions de sécurité".*

Cette présentation pourrait également faire une description de la typologie des clients du candidat (exemple: service proposé exclusivement aux établissements de santé, pas d'accès direct aux données pour les patients, ...). Par la suite, le candidat pourrait décrire sommairement les fonctions essentielles de son système (fonctions opérationnelles, fonctions de support, fonctions de contrôle).

Le candidat est tenu d'indiquer, pour la localisation du service d'hébergement, les adresses des différents sites concourant à la réalisation du service d'hébergement. Une courte explication sur le rôle de ces sites est appréciée.

Les adresses des sites des sous-traitants doivent également être renseignées, ainsi que les informations demandées pour les sous-traitants (formulaire P2).

Exemple:

Notre service d'hébergement de l'application "*Santé1*" repose sur une architecture bi-site actif/passif. Notre site principal d'exploitation est situé à Paris et notre site de secours est situé à Nice. Nos deux sites sont reliés par une liaison dédiée et redondée.

Le candidat est tenu de préciser les noms, fonctions, qualifications et les liens contractuels qui le lient avec les personnes chargés (les opérateurs) de mettre en œuvre le service d'hébergement sur le périmètre concerné par la demande d'agrément.

Les activités du candidat peuvent l'amener à réaliser différentes prestations d'hébergement de données. Le candidat doit donc préciser les informations relatives au personnel chargé de mettre en œuvre le service d'hébergement de données de santé uniquement.

➢ Les liens de télécommunications

Dans ce chapitre, il est principalement attendu du candidat une présentation des liens de communication suivants:

- liens de communication entre les sites du candidat (voire, de ses sous-traitants)

- liens de communication entre le système central et les clients du candidat

- liens de communication au sein du système d'information du candidat.

Il est recommandé de préciser pour chacun de ces types de liens les protocoles mis en oeuvre ainsi que les moyens de sécurité associés.

Le candidat peut également préciser si les données sont chiffrées lors de leur transport.

➢ La gestion des incidents

Le candidat est invité à décrire les moyens mis en œuvre, afin d'assurer la gestion des incidents. Pour ce faire, il est recommandé aux candidats de décrire les modalités de retour d'expérience faisant suite aux incidents passés résolus. Un processus de veille sécurité peut également être décrit.

En outre, les informations relatives aux processus de contrôles de conformité à sa PSSI, le candidat peut présenter dans ce chapitre s'il dispose d'un processus de veille réglementaire ou juridique lui permettant de s'assurer de sa conformité avec la législation en vigueur sur son périmètre d'activité.

Les mécanismes de traçabilité doivent être précisés par le candidat.

Les dispositifs de gestion des traces ne peuvent pas être optionnels.

F – LES SUITES DE L'AGRÉMENT

Une auto-évaluation doit être adressée tous les ans par les organismes agréés en qualité d'hébergeurs. Elle a pour objet d'informer des changements intervenus au cours de l'année écoulée. Si l'auto-évaluation remet en cause le périmètre de l'agrément initial l'organisme devra déposer une nouvelle demande d'agrément.

Une association créée en 2010 par les premiers organismes agréés hébergeurs de données de santé à caractère personnel (AFHADS) se réunit régulièrement pour partager les expériences et parvenir à des interprétations communes tout en nourrissant la réflexion sur les évolutions possibles de la procédure. Au-delà de la simple défense des intérêts de ces organismes, cette association travaille en concertation avec l'ASIP Santé pour intégrer la réflexion dans le champ plus large de la politique de sécurité des systèmes information de santé.

TITRE 6 : BILAN ET PERSPECTIVES

Les dossiers montrent une grande diversité d'activités et de compétences derrière celle d'hébergement des données de santé.

Cette diversité tient à la variété de positionnement dans la chaîne des valeurs des services d'information : de la salle blanche jusqu'à la prestation de service aux patients en passant par l'exploitation des machines, des sites, des sauvegardes, l'intégration de service, les communications…

Certains déclarants portent le dossier en se plaçant en amont de cette chaîne (infrastructure) ou en aval (service aux patients). D'autres candidats assurent plusieurs fonctions simultanément. D'autres enfin se positionnent comme intégrateurs de divers sous-traitants qui assurent des fonctions élémentaires et/ou comme fournisseur de la prestation finale délivrée à un établissement de santé ou aux patients.

Une autre source de diversité provient des prestations de service elles-mêmes. Celles-ci n'ont en commun que la fonction d'hébergement, et concernent par ailleurs tous types de traitements à l'usage de praticiens, d'établissements, de réseaux de santé, d'institutions –ou des patients eux-mêmes.

La tâche d'instruction permet de s'assurer de la conformité du dossier du candidat aux exigences légales et réglementaires. Mais ceci ne peut se faire qu'avec une compréhension suffisante des enjeux, modalités, risques associés à la prestation particulière. En effet, avec l'expérience, l'idée d'une typologie de prestation semble incompatible avec l'évolution rapide des technologies et des besoins du marché. C'est pourquoi le respect des éléments suivants est impératif et reçoit toute l'attention du comité d'agrément.

La question de l'architecture générale est une question-clé, ainsi que celle de la place de la fonction d'hébergement dans l'ensemble de la prestation de service. Ceci vaut pour le candidat lui-même, mais aussi pour ses sous-traitants, qui contribuent à la prestation d'ensemble. Or, les relations entre les sites, les fonctions qu'ils supportent, sont bien souvent incomplètement décrites, ce qui rend l'instruction difficile.

Corrélativement, les personnels en situation d'accéder aux données de santé, et dont l'activité est porteuse de risques au niveau de la confidentialité, sont rarement identifiés de façon convenable.

Le comité d'agrément est conscient que les évolutions technologiques, comme le "*Cloud computing*", les infrastructures "*as a service*" rendront de plus en plus difficile dans le futur l'application d'une réglementation appuyée sur une description des ressources. Mais, dans le même temps, c'est à partir des limites et des exigences du décret actuel que s'élaborera la nouvelle doctrine, pour peu que les dossiers déposés soient clairs et complets.

S'agissant enfin des dispositions de sécurité, celles-ci concernent le respect des droits des personnes, le contrôle d'accès, les télécommunications, la gestion des incidents, la conformité à un Plan de Politique de Sécurité des Systèmes d'information (PSSI). Le comité doit s'assurer du respect de ces dispositions, quelle que soit la complexité du montage technique et organisationnel proposé. Un des éléments de la doctrine émergente concerne par exemple la responsabilité du candidat vis-à-vis de la traçabilité des accès, même s'il n'est pas en situation de l'assurer lui-même. Une responsabilité collective s'établit en effet à ce niveau. Le candidat ne peut s'affranchir des siennes propres et doit montrer comment il s'assure de façon contractuelle et dans son mode de relation que les exigences réglementaires à ce niveau sont respectées.

Il est à signaler que le comité, soucieux de pragmatisme, constate la diffusion encore limitée des cartes CPS et salue donc les travaux entrepris par l'ASIP Santé pour diffuser de façon systématique cette carte dès lors que l'identité du professionnel de santé a été certifiée dans le RPPS. Dans l'attente d'une diffusion généralisée, il admet des réponses se référant à une authentification forte. Le cryptage total des données, s'il constitue une réponse de haut niveau de sécurité, ne peut-être la seule réponse selon le type de service et l'impact économique qui peut en résulter le cas échéant. Le comité a indiqué à la CNIL toute l'importance qu'il accorde à la doctrine en cours d'élaboration par cette instance en concertation avec l'ASIP Santé, autorité en charge de la définition des référentiels de sécurité pour le partage des données de santé à caractère personnel et son intention d'adopter une position convergente.

TITRE 7 : CONCLUSION

L'obligation de recevoir un agrément ministériel pour exercer une activité d'hébergement de données de santé à caractère personnel pour des tiers a été ressentie positivement par les professionnels de santé et les associations de patients. L'encadrement a permis d'élever le niveau général des prestations proposées et en développant des référentiels de qualité, d'éviter la pollution du marché par des acteurs n'offrant pas des garanties suffisantes. Les acteurs de l'hébergement se regroupent ainsi en une Association Française des Hébergeurs Agréés de Données de Santé à Caractère Personnel.

On peut toutefois s'interroger sur le type d'écosystème qui va se mettre en place si les procédures d'agrément se complexifient, l'activité d'hébergement pourrait alors être réservée aux sociétés industrielles de grande taille, qui finiraient par être très éloignées du patient et donc peu sensibilisées aux aspects spécifiques aux données de santé.

L'agrément repose sur une procédure d'instruction lourde. L'expertise menée en parallèle par l'ASIP Santé et la CNIL porte en partie sur des points identiques. Elle génère ainsi des coûts humains et financiers importants. Le souci de stricte économie dans la gestion des fonds publics impose donc une révision du référentiel afin d'éviter des redondances. En outre, le respect des délais prévus par les textes se heurte à la nécessité de se soumettre à la double contrainte des dates de réunion du Comité et des dates de séances de la CNIL. Ces raisons justifient un allégement de la procédure pour la rendre plus fluide.

La deuxième période quinquennale d'activité a été ouverte par la publication de l'arrêté du 14 juin 2011 nommant les membres du nouveau comité. Outre sa tâche spécifique de rendre des avis d'agrément destinés au ministre, ce nouveau comité s'efforcera de fournir aux pouvoirs publics les éléments leur permettant de trancher entre deux évolutions possibles :

- une réécriture du décret du 4 janvier 2006 qui pourrait aménager le référentiel dans le but d'éviter des redondances avec les instructions menées par la CNIL et de permettre l'adaptation aux évolutions technologiques ;
- une procédure de certification type Cofrac. Le Comité d'Agrément statuera alors au vu de rapports établis par des évaluateurs privés et dont les coûts d'instruction seront supportés par les candidats.

Le Comité d'agrément a demandé au Président de la CNIL d'associer son institution au groupe de travail qui se mettra en place au dernier trimestre 2011.

Les évolutions technologiques, particulièrement la diffusion de l'informatique en nuage, interpellent les pouvoirs publics en raison entre autres des dangers encourus par la sécurité nationale. Les données de santé agrégées ou individuelles représentent des enjeux économiques et de confidentialité majeurs. Le Comité demandera à être entendu par les commissions gouvernementales travaillant sur cette problématique.

Le périmètre des activités d'hébergement soumis à l'agrément doit être clarifié, en particulier concernant les bases de données de l'Assurance Maladie. La Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés – CNAMTS - met à la disposition des Echelons Locaux du Service Médical un traitement automatisé de données nominatives, le système Hippocrate. Ce traitement héberge des données à caractère personnel recueillies à l'occasion d'activités de soins, de diagnostic et de prévention. Il est juste de s'interroger sur les obligations de l'hébergeur du système Hippocrate au regard de la procédure d'agrément.

Il paraît également indispensable que le Comité d'agrément soit informé des incidents et dysfonctionnements survenus chez les hébergeurs ou constatés lors de contrôles. C'est ainsi qu'il sera mieux à même d'exercer sa vigilance sur la cohérence des déclarations faites par les hébergeurs lors de leur demande d'agrément. Le Comité a donc demandé au Président de la CNIL de participer à certains contrôles que la Commission diligente, bien évidemment dans le respect strict des procédures de la CNIL. La même demande a été adressée au chef de l'inspection générale des affaires sociales en charge des contrôles de sa responsabilité.

Enfin, la procédure d'agrément qui permet de décliner des exigences déontologique et techniques pourrait être discutée au sein du Groupe de l'article 29 rassemblant les autorités de protection des données exerçant dans les Etats membres de l'Union européenne ; Un agrément européen permettrait aux industriels de se porter candidat pour héberger des dossiers partagés européens (EPsos).

LES RECOMMANDATIONS DU COMITÉ D'AGRÉMENT EN 8 POINTS

1) Les candidats doivent déposer un dossier de demande d'agrément identifiant clairement un type de prestation.

2) Lorsque le candidat reçoit des financements publics, l'Agence Régionale de Santé dont il dépend pourrait fournir au CAH les informations budgétaires prévisionnelles et les informations sur le maintien du financement.

3) Lorsque l'agrément est prononcé et qu'un courrier de recommandations est adressé au candidat, il faut prévoir un suivi de ces recommandations et le Comité d'agrément devrait être informé de tous les incidents survenant au cours de l'hébergement créant un risque pour la confidentialité et la sécurité des données. Il devra en informer la CNIL. Il est demandé à la CNIL d'effectuer la même démarche lorsqu'elle constate des incidents.

4) L'hébergeur agréé devrait recevoir de ses clients une déclaration annuelle des moyens que ces derniers mettent en œuvre pour assurer l'information des patients et des professionnels.

5) L'hébergeur doit être responsable de l'information dispensée à ses clients sur les points suivants :

- maintien du caractère opérationnel des dispositifs d'encodage ;

- informations précises sur les conséquences d'une interruption du service prenant en compte les capacités et caractéristiques informatiques du client ;

- informations sur la durée de conservation des données selon les différents supports utilisés et mise en place d'une information d'alerte lorsque la durée de conservation va être atteinte de telle sorte que les clients puissent mettre en place avec l'hébergeur les solutions appropriées.

6) Le Comité d'agrément doit réfléchir à l'adaptation de la procédure en concertation avec la CNIL et l'ASIP Santé, en particulier vers un système de certification.

7) La réécriture du décret devrait permettre de prendre en compte les évolutions technologiques.

8) Les relations entre l'hébergeur et les sous-traitants ; les garanties offertes par les sous-traitants doivent être décrites.

LE POINT DE VUE DE NATHALIE TELLIER, MEMBRE DU COMITÉ D'AGRÉMENT AU TITRE DES ASSOCIATIONS COMPÉTENTES EN MATIÈRE DE SANTÉ

Le CISS siège au titre des associations agréées compétentes en matière de santé avec voix délibérative.

Comme tout membre du comité les représentants du CISS ont à examiner l'ensemble des dossiers de demande d'agrément et sont rapporteurs de certains.

Il est tout à fait essentiel que les représentants des familles et des patients siègent dans ce comité car lorsque par exemple le patient consent à l'ouverture d'un dossier médical informatisé destiné à recevoir des données de santé à caractère personnel, il consent également à l'hébergement de ces données.

Les associations siégeant au sein du comité sont donc tout particulièrement attentives au respect des libertés publiques et des droits de la personne.

Dans le dossier de demande d'agrément une large partie est consacrée au respect des droits des personnes et à la sécurité de l'accès aux informations.

Ainsi le candidat à l'hébergement doit notamment indiquer dans son dossier comment et qui recueille le consentement, quelles sont les modalités d'accès aux données de santé, comment est assurée la traçabilité des actions effectuées, quels sont les moyens d'identification, d'authentification et de contrôle d'accès. Le client doit enfin garantir la confidentialité, l'intégrité et la pérennité des données.

Tous ces points sont essentiels car parler d'hébergement de données de santé, c'est parler de sécurité des données stockées et/ou échangées.

Lors de l'ouverture de dossiers informatisés en matière de santé, il est tout fait essentiel que la personne ait conscience qu'elle consent également à l'hébergement des données. Ce point est inscrit dans le document matérialisant l'information lors de l'ouverture d'un dossier pharmaceutique et d'un DMP. Mais qu'en est-il des autres dossiers ? Il paraît que sur ce point les usages divergent.

Car force est de constater aujourd'hui que l'information en matière d'hébergement des données de santé est trop souvent pas ou peu faite. Lors d'une hospitalisation, la personne sait-elle que ses données médicales sont hébergées par telle ou telle société agréée ?

Pourtant, une information préalable est nécessaire.

Les hébergeurs et les candidats doivent être sensibilisés sur ce point, une information au moment du recueil du consentement est incontournable si l'on veut que les personnes comprennent ce qu'est l'hébergement des données de santé.

ANNEXE 1 : DÉCRET N°2006-6 DU 4 JANVIER 2006 RELATIF A L'HÉBERGEMENT DE DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL ET MODIFIANT LE CODE DE LA SANTÉ PUBLIQUE (DISPOSITIONS RÈGLEMENTAIRES)

JORF n°4 du 5 janvier 2006 page 174
texte n° 14

DECRET

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 (dispositions réglementaires)

NOR: SANX0500308D

Le Président de la République,
Sur le rapport du Premier ministre et du ministre de la santé et des solidarités,
Vu le code du patrimoine, notamment le titre Ier du livre II ;
Vu le code de la santé publique, notamment ses articles L. 1111-7, L. 1111-8 et L. 1112-1 ;
Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
Vu la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, notamment ses articles 21 et 24 ;
Vu le décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques ;
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 l'avis du Conseil national de l'ordre des médecins en date du 1er avril 2004 ;
Vu l'avis du Conseil national de l'ordre des chirurgiens-dentistes en date du 8 avril 2004 ;
Vu l'avis du Conseil national de l'ordre des pharmaciens en date du 11 mai 2004 ;
Vu l'avis du Conseil national de l'ordre des sages-femmes en date du 26 mai 2004 ;
Vu les avis de la Commission nationale de l'informatique et des libertés en date des 27 mai 2004 et 15 mars 2005 ;
Le Conseil d'Etat (section sociale) entendu ;
Le conseil des ministres entendu,

Décrète :

Article 1 En savoir plus sur cet article...

Le chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique (dispositions réglementaires) est ainsi modifié :
I. - La section unique devient la sous-section 1, intitulée *« Sous-section 1 : Accès aux informations de*

santé à caractère personnel », au sein d'une section 1 dont le titre est ainsi rédigé :
« Section 1

« Principes généraux »

II. - Après l'article R. 1111-8, il est ajouté une sous-section 2 ainsi rédigée :

« Sous-section 2

« Hébergement des données de santé à caractère personnel

« Art. R. 1111-9. - Toute personne physique ou morale souhaitant assurer l'hébergement de données de santé à caractère personnel, mentionné à l'article L. 1111-8, et bénéficier d'un agrément à ce titre doit remplir les conditions suivantes :
« 1° Offrir toutes les garanties pour l'exercice de cette activité, notamment par le recours à des personnels qualifiés en matière de sécurité et d'archivage des données et par la mise en oeuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données confiées, ainsi qu'un usage conforme à la loi;
« 2° Définir et mettre en oeuvre une politique de confidentialité et de sécurité, destinée notamment à assurer le respect des exigences de confidentialité et de secret prévues par les articles L. 1110-4 et L. 1111-7, la protection contre les accès non autorisés ainsi que la pérennité des données, et dont la description doit être jointe au dossier d'agrément dans les conditions fixées par l'article R. 1111-14 ;
« 3° Le cas échéant, identifier son représentant sur le territoire national au sens de l'article 5 de la loi du 6 janvier 1978 ;
« 4° Individualiser dans son organisation l'activité d'hébergement et les moyens qui lui sont dédiés, ainsi que la gestion des stocks et des flux de données ;
« 5° Définir et mettre en place des dispositifs d'information sur l'activité d'hébergement à destination des personnes à l'origine du dépôt, notamment en cas de modification substantielle des conditions de réalisation de cette activité ;
« 6° Identifier les personnes en charge de l'activité d'hébergement, dont un médecin, en précisant le lien contractuel qui les lie à l'hébergeur.
« Art. R. 1111-10. - L'agrément nécessaire à l'activité d'hébergement de données de santé à caractère personnel est délivré par le ministre chargé de la santé, qui se prononce après avis de la Commission nationale de l'informatique et des libertés et d'un comité d'agrément placé auprès de lui.*
« A cet effet, la personne intéressée adresse au ministre chargé de la santé un dossier de demande d'agrément comprenant les éléments mentionnés à l'article R. 1111-12. Le ministre transmet le dossier à la Commission nationale de l'informatique et des libertés, qui apprécie les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données. La commission rend son avis dans un délai de deux mois à compter de la réception du dossier, délai pouvant être renouvelé une fois sur décision motivée de son président.
« Dès que la commission s'est prononcée ou à l'expiration du délai qui lui était imparti, elle transmet la demande d'agrément, accompagnée, le cas échéant, de son avis, au comité d'agrément mentionné au premier alinéa. Ce comité se prononce sur tous les aspects du dossier, en particulier sur les garanties d'ordre éthique, déontologique, technique, financier et économique qu'offre le candidat. Il émet son avis dans le mois qui suit la réception du dossier transmis par la Commission nationale de l'informatique et des libertés. Il peut toutefois demander un délai supplémentaire d'un mois.

« Le ministre chargé de la santé dispose, pour prendre sa décision, d'un délai de deux mois suivant l'avis du comité d'agrément. A l'issue de ce délai, son silence vaut décision de rejet.
« Art. R. 1111-11. - I. - Le comité d'agrément mentionné à l'article R. 1111-10 comprend :
« 1° Un membre de l'inspection générale des affaires sociales nommé sur proposition du chef de l'inspection générale des affaires sociales ;
« 2° Deux représentants des associations compétentes en matière de santé, agréées au niveau national dans les conditions prévues à l'article L. 1114-1 ;
« 3° Deux représentants des professions de santé, l'un nommé sur proposition du Conseil national de l'ordre des médecins et l'autre sur proposition de l'Union nationale des professions de santé ;
« 4° Trois personnalités qualifiées :
« a) Une personne choisie en raison de ses compétences dans les domaines de l'éthique et du droit ;
« b) Une personne choisie en raison de ses compétences en matière de sécurité des systèmes d'information et de nouvelles technologies ;
« c) Une personne choisie en raison de ses compétences dans le domaine économique et financier.
« Le directeur général de la santé, le directeur de l'hospitalisation et de l'organisation des soins, le directeur des Archives de France, le directeur général des entreprises et le directeur général de la concurrence, de la consommation et de la répression des fraudes, ou leurs représentants, assistent aux séances du comité avec voix consultative.
« II. - Les membres du comité d'agrément, dont celui qui, parmi eux, exercera la présidence du comité, sont nommés pour cinq ans par arrêté du ministre chargé de la santé. Leur mandat est renouvelable une fois.
« Lors de leur entrée en fonction, les membres du comité adressent au président une déclaration mentionnant toute activité personnelle ou professionnelle en rapport direct ou indirect avec les missions du comité, ainsi que les liens directs ou indirects qu'ils peuvent avoir avec tout organisme hébergeant ou susceptible d'héberger des données de santé à caractère personnel ou avec les organismes professionnels et les sociétés de conseil intervenant dans le domaine de compétence du comité. Ils s'engagent à signaler toute modification concernant cette situation.
« Ils ne peuvent siéger lorsque est examinée une affaire relative à un organisme au sein duquel ils détiennent un intérêt, exercent des fonctions ou détiennent un mandat, ou au sein duquel ils ont, au cours des dix-huit mois précédant la séance, détenu un intérêt, exercé des fonctions ou détenu un mandat.
« Des suppléants en nombre égal au nombre de titulaires sont désignés dans les mêmes conditions que ceux-ci. Un membre titulaire empêché ou intéressé par une affaire est remplacé par son suppléant.
« Le remplacement d'un membre du comité en cas de cessation de fonction en cours de mandat est réalisé dans les mêmes conditions que sa nomination et pour la durée du mandat restant à courir.
« Les fonctions de membre du comité ouvrent droit à des indemnités pour frais de déplacement et de séjour dans les conditions prévues par les dispositions législatives et réglementaires applicables aux fonctionnaires civils de l'Etat.
« III. - Le comité d'agrément ne peut délibérer que si deux tiers au moins de ses membres sont présents. Dans le cas contraire, une nouvelle séance peut se tenir sans obligation de quorum après un délai de quinze jours.
« Les avis rendus par le comité sont motivés. Ils sont pris à la majorité des voix exprimées des membres présents. En cas de partage égal des voix, celle du président est prépondérante.
« IV. - Le comité d'agrément peut être saisi par le ministre chargé de la santé de tout sujet entrant

dans son domaine de compétence.
« Art. R. 1111-12. - Le dossier de demande d'agrément comprend les éléments suivants :
« 1° L'identité et l'adresse du responsable du service d'hébergement et, le cas échéant, de son représentant ; pour les personnes morales, les statuts sont produits ;
« 2° Les noms, fonctions et qualifications des opérateurs chargés de mettre en oeuvre le service, ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont accès aux données hébergées ;
« 3° L'indication des lieux dans lesquels sera réalisé l'hébergement ;
« 4° Une description du service proposé ;
« 5° Les modèles de contrats devant être conclus, en application du deuxième alinéa de l'article L. 1111-8, entre l'hébergeur de données de santé et les personnes physiques ou morales qui sont à l'origine du dépôt des données de santé à caractère personnel ; ces modèles sont établis conformément aux dispositions de l'article R. 1111-13 ;
« 6° Les dispositions prises pour assurer la sécurité des données et la garantie des secrets protégés par la loi, notamment la présentation de la politique de confidentialité et de sécurité prévue au 2° de l'article R. 1111-9 ;
« 7° Le cas échéant, l'indication du recours à des prestataires techniques externes et les contrats conclus avec eux ;
« 8° Un document présentant les comptes prévisionnels de l'activité d'hébergement et, éventuellement, les trois derniers bilans et la composition de l'actionnariat du demandeur, ainsi que, dans le cas d'une demande de renouvellement, les comptes de résultat et bilans liés à cette activité d'hébergement depuis le dernier agrément.
« L'hébergeur déjà agréé informe sans délai le ministre chargé de la santé de tout changement affectant les informations mentionnées ci-dessus et de toute interruption, temporaire ou définitive, de son activité.
« Art. R. 1111-13. - Les modèles de contrats devant être joints à la demande d'agrément, mentionnés au 5° de l'article R. 1111-12, contiennent obligatoirement au moins les clauses suivantes :
« 1° La description des prestations réalisées : contenu des services et résultats attendus ;
« 2° Lorsque le contrat est souscrit par la personne concernée par les données hébergées, la description des modalités selon lesquelles les professionnels de santé et les établissements de santé les prenant en charge et désignés par eux peuvent être autorisés à accéder à ces données ou en demander la transmission et l'indication des conditions de mise à disposition de ces données ;
« 3° Lorsque le contrat est souscrit par un professionnel de santé ou un établissement de santé, la description des modalités selon lesquelles les données hébergées sont mises à leur disposition, ainsi que les conditions de recueil de l'accord des personnes concernées par ces données s'agissant tant de leur hébergement que de leurs modalités d'accès et de transmission ;
« 4° La description des moyens mis en oeuvre par l'hébergeur pour la fourniture des services ;
« 5° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, ainsi que de la périodicité de leur mesure ;
« 6° Les obligations de l'hébergeur à l'égard de la personne à l'origine du dépôt des données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ;
« 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 équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement ;
« 8° Une information sur les garanties permettant de couvrir toute défaillance éventuelle de

l'hébergeur ;
« 9° Une présentation des prestations à la fin de l'hébergement.
« Art. R. 1111-14. - Une présentation de la politique de confidentialité et de sécurité, prévue au 2° de l'article R. 1111-9, doit être fournie à l'appui de la demande d'agrément conformément au 6° de l'article R. 1111-12. Elle comporte notamment les précisions suivantes :
« 1° En matière de respect des droits des personnes concernées par les données hébergées :
« a) Les modalités permettant de s'assurer de l'existence du consentement de l'intéressé à l'hébergement des données le concernant ;
« b) Les modalités retenues pour que l'accès aux données de santé à caractère personnel et leur transmission éventuelle n'aient lieu qu'avec l'accord des personnes concernées et par les personnes désignées par elles ;
« c) Les conditions dans lesquelles sont présentées et prises en compte les éventuelles demandes de rectification des données de santé à caractère personnel hébergées ;
« d) Les moyens mis en oeuvre pour assurer le respect des dispositions de l'article L. 1111-7 relatif à l'accès des personnes à leurs informations de santé, notamment en termes de délais et de modalités de consultation ;
« e) Les procédures de signalement des incidents graves, dont l'altération des données ou la divulgation non autorisée des données personnelles de santé ;
« f) La fourniture à la personne concernée par les données hébergées, à sa demande, de l'historique des accès aux données et des consultations ainsi que du contenu des informations consultées et des traitements éventuellement opérés.
« 2° En matière de sécurité de l'accès aux informations :
« a) Les dispositions prises pour garantir la sécurité des accès et des transmissions des données de santé à caractère personnel vis-à-vis des établissements ou des professionnels de santé à l'origine du dépôt et des personnes concernées par ces données ;
« b) Les mesures prises en matière de contrôle des droits d'accès et de traçabilité des accès et des traitements ;
« c) Les conditions de vérification du contenu des traces des accès et des traitements afin de détecter les tentatives d'effraction ou d'accès non autorisés ;
« d) Les modalités de vérification du registre des personnes habilitées à accéder aux données hébergées tenant compte des éventuelles mises à jour ;
« e) Les procédés techniques retenus en matière d'identification et d'authentification ; en ce qui concerne les professionnels de santé, ces procédés techniques doivent avoir été agréés par le groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale.
« 3° En matière de pérennité des données hébergées :
« a) Les procédures visant à assurer, au moment du transfert des données vers l'hébergeur, la réception sécurisée des données et l'intégrité de celles-ci, leur prise en compte dans le système d'information de l'hébergeur et le suivi de cette prise en charge ;
« b) Les modalités de prise en compte et d'enrichissement tout au long de la durée de l'hébergement, de l'ensemble des informations concernant les données depuis leur création, telles que les données permettant de les identifier et de les décrire, de les gérer, de déterminer leurs propriétés techniques et d'en assurer la traçabilité ;
« c) Les modalités de surveillance des supports en vue d'anticiper les changements technologiques et, le cas échéant, d'opérer des migrations de supports dans des conditions en garantissant la traçabilité;

« d) Les procédures liées à la réplication des données sur différents supports informatiques en des lieux distincts ;
« e) Les conditions de mise en oeuvre d'une alerte concernant les formats d'encodage des données, destinée à avertir la personne à l'origine du dépôt en cas d'obsolescence de ce format et, éventuellement, les procédures visant à réaliser, avec l'autorisation de la personne à l'origine du dépôt, des migrations de formats des données, si ces derniers ne permettent plus d'assurer la lisibilité des informations et à assurer la traçabilité de ces migrations.
« 4° En matière d'organisation et de procédures de contrôle interne en vue d'assurer la sécurité des traitements et des données :
« a) La désignation d'un responsable sécurité et d'un responsable qualité ;
« b) La définition des missions, des pouvoirs et des obligations des personnels de l'hébergeur et de ses éventuels sous-traitants, habilités à traiter les données de santé à caractère personnel ;
« c) Les spécifications techniques des logiciels et des mécanismes de sécurité propres à garantir la confidentialité des transmissions, notamment en ce qui concerne le mode de chiffrement des flux d'information ;
« d) Les modalités retenues pour l'évaluation périodique des risques et l'audit des mesures de protection mises en place afin de garantir la sécurité des données et en vue d'apporter les modifications nécessaires en cas de détection de défaillances ;
« e) Les dispositifs de simulation régulière de défauts de fonctionnement pour vérifier l'efficacité des mécanismes destinés à garantir la continuité des services ;
« f) Les moyens mis en oeuvre pour sensibiliser et former le personnel aux mesures de protection mises en place et à leurs obligations en matière de confidentialité et de respect du secret professionnel ;
« g) Les conditions de mise en oeuvre de la sécurité physique des sites informatiques, des mesures de protection de l'infrastructure technique, notamment en termes de sécurité des réseaux, des serveurs et des postes de travail ;
« h) Les dispositions prises en ce qui concerne l'exploitation de l'infrastructure technique ;
« i) Les conditions de mise en oeuvre du plan de secours informatique comportant notamment les dispositions prises pour informer du déclenchement de ce plan les personnes physiques ou morales à l'origine du dépôt des données de santé à caractère personnel ainsi que les dispositions prises pour la reprise des activités.
« Art. R. 1111-15. - L'agrément est délivré aux hébergeurs de données de santé à caractère personnel pour une durée de trois ans.
« La demande de renouvellement doit être déposée au plus tard six mois avant le terme de la période d'agrément. Elle comprend les documents mentionnés au 8° de l'article R. 1111-12 et un récapitulatif des modifications intervenues depuis la dernière demande d'agrément en ce qui concerne les autres documents mentionnés à cet article, ainsi qu'un audit externe réalisé aux frais de l'hébergeur, attestant de la mise en oeuvre de la politique de confidentialité et de sécurité mentionnée à l'article R. 1111-14. Elle est instruite selon la même procédure que celle applicable à la demande initiale.
« Les décisions d'agrément, ainsi que le renouvellement de cet agrément, sont publiées au Bulletin officiel du ministère de la santé.
« Art. R. 1111-16. - Le ministre chargé de la santé, lorsqu'il envisage de procéder au retrait d'un agrément en application du quatrième alinéa de l'article L. 1111-8, communique à l'hébergeur intéressé, par lettre recommandée avec demande d'avis de réception, les motifs de ce projet de retrait et l'appelle à formuler ses observations, écrites ou, à sa demande, orales, dans un délai de deux mois.

« En cas de divulgation non autorisée de données de santé à caractère personnel ou de manquements graves de l'hébergeur à ses obligations mettant notamment en cause l'intégrité, la sécurité et la pérennité des données hébergées, le ministre chargé de la santé peut, à titre conservatoire, dans l'attente qu'il soit statué définitivement sur le projet de retrait d'agrément, prononcer la suspension de l'activité d'hébergement.
« La décision de retrait est notifiée à l'hébergeur intéressé, par lettre recommandée avec demande d'avis de réception. Elle met fin de plein droit à l'hébergement des données confiées à l'hébergeur et entraîne la restitution de ces données aux personnes ayant contracté avec l'hébergeur.
« Les décisions de suspension et de retrait font l'objet de la mesure de publicité prévue à l'article R. 1111-15. Elles sont transmises pour information au comité d'agrément mentionné à l'article R. 1111-10 ainsi qu'à la Commission nationale de l'informatique et des libertés. »

Article 2 En savoir plus sur cet article...

I. - Après le premier alinéa de l'article R. 1111-2 du code de la santé publique, il est inséré un alinéa ainsi rédigé :
« Dans le cas où les informations demandées sont détenues par un établissement de santé et si les dispositifs techniques de l'établissement le permettent, le demandeur peut également consulter par voie électronique tout ou partie des informations en cause. »
II. - L'article R. 1112-7 du même code est remplacé par les dispositions suivantes :
« Art. R. 1112-7. - Les informations concernant la santé des patients sont soit conservées au sein des établissements de santé qui les ont constituées, soit déposées par ces établissements auprès d'un hébergeur agréé en application des dispositions à l'article L. 1111-8.
« Le directeur de l'établissement veille à ce que toutes dispositions soient prises pour assurer la garde et la confidentialité des informations ainsi conservées ou hébergées.
« Le dossier médical mentionné à l'article R. 1112-2 est conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein. Lorsqu'en application des dispositions qui précèdent, la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date. Dans tous les cas, si la personne titulaire du dossier décède moins de dix ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de dix ans à compter de la date du décès. Ces délais sont suspendus par l'introduction de tout recours gracieux ou contentieux tendant à mettre en cause la responsabilité médicale de l'établissement de santé ou de professionnels de santé à raison de leurs interventions au sein de l'établissement.
« A l'issue du délai de conservation mentionné à l'alinéa précédent et après, le cas échéant, restitution à l'établissement de santé des données ayant fait l'objet d'un hébergement en application de l'article L. 1111-8, le dossier médical peut être éliminé. La décision d'élimination est prise par le directeur de l'établissement après avis du médecin responsable de l'information médicale. Dans les établissements publics de santé et les établissements de santé privés participant à l'exécution du service public hospitalier, cette élimination est en outre subordonnée au visa de l'administration des archives, qui détermine ceux de ces dossiers dont elle entend assurer la conservation indéfinie pour des raisons d'intérêt scientifique, statistique ou historique. »
III. - Le délai de conservation des dossiers médicaux fixé à l'article R. 1112-7 du code de la santé publique s'appliquera à l'issue d'un délai de douze mois suivant la publication du présent décret.

Article 3 En savoir plus sur cet article...

Au 2 du titre II de l'annexe au décret n° 97-1185 du 19 décembre 1997, le tableau intitulé *« code de la santé publique »* est ainsi complété :

Vous pouvez consulter le tableau dans le JO n° 4 du 05/01/2006 texte numéro 14

Article 4 En savoir plus sur cet article...

Les dispositions du présent décret peuvent être modifiées par décret en Conseil d'Etat, à l'exception de celles qui déterminent la compétence du ministre chargé de la santé figurant à l'article R. 1111-10 du code de la santé publique et de celles de l'article 3 du présent décret dont la modification ne peut intervenir que dans les conditions prévues à l'article 2 du décret du 15 janvier 1997.*

Article 5 En savoir plus sur cet article...

Le Premier ministre, le ministre de la santé et des solidarités et le ministre de la culture et de la communication 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 à Paris, le 4 janvier 2006.

Jacques Chirac

Par le Président de la République :

Le Premier ministre,

Dominique de Villepin

Le ministre de la santé et des solidarités,

Xavier Bertrand

Le ministre de la culture et de la communication,

Renaud Donnedieu de Vabres

MISE À JOUR

L'article 1er du décret n°2011-246 du 4 mars 2011 relatif à l'hébergement de données de santé à caractère personnel sur support papier complète les dispositions du décret 2006-6 du 4 janvier 2006 en ajoutant après les mots *« hébergement de données de santé à caractère personnel »* « sur support informatique », et modifie la codification des articles du code de la santé publique issus du décret 2006-6 du 4 janvier 2006 (sans modification de contenu) : l'ancien article R 1111-16 du code de la santé publique devient l'article R 1111-15-1 du code de la santé publique.

Article 1er du décret n°2011-246 du 4 mars 2011 :

I. — A l'intitulé de 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, après les mots : *« Hébergement des données de santé à caractère personnel »,*

sont ajoutés les mots : *« sur support informatique ».*

L'article R. 1111-16 devient l'article R. 1111-15-1.

II. — Au premier alinéa de l'article R. 1111-9, après les mots : *« données de santé à caractère personnel »,*

sont ajoutés les mots : *« sur support informatique ».*

III. — Au premier alinéa de l'article R. 1111-10, après les mots : *« données de santé à caractère personnel »*,

sont ajoutés les mots : *« sur support informatique ».*

IV. — Au premier alinéa de l'article R. 1111-15, après les mots : *« données de santé à caractère personnel »*,

sont ajoutés les mots : *« sur support informatique ».*

V. — Au deuxième alinéa de l'article R. 1111-15-1, après les mots *: « données de santé à caractère personnel »,*

sont ajoutés les mots : *« sur support informatique ».*

Annexes 2

ARRÊTÉ DU 7 FÉVRIER 2006 FIXANT LA COMPOSITION DU COMITÉ D'AGRÉMENT DES HÉBERGEURS DE DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL

JORF n°39 du 15 février 2006
Texte n°71

ARRETE
Arrêté du 7 février 2006 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel

NOR: SANP0620592A

« Par arrêté du ministre de la santé et des solidarités en date du 7 février 2006, sont nommés pour cinq ans membres du comité d'agrément des hébergeurs de données de santé à caractère personnel :

Au titre de l'inspection générale des affaires sociales

M. Daniel POSTEL-VINAY, titulaire, et M. Christophe LANNELONGUE, suppléant ;

Au titre des associations d'usagers compétentes en matière de santé et agréées

MM. Jean-Luc BERNARD et Christian SAOUT, titulaires,
M. le docteur Michel DELCEY et Mme Anne LAZAREVITCH, suppléants ;

Au titre du Conseil national de l'ordre des médecins

M. le docteur Philippe BICLET, titulaire, et M. le docteur Jean-Jacques KENNEL, suppléant ;

Au titre de l'Union nationale des professions de santé

M. le docteur Gérard GALLIOT, titulaire, et M. Patrick CORNE, suppléant ;

Au titre de personnalités qualifiées

Dans les domaines de l'éthique et du droit :
M. Gilles BARDOU, titulaire, et Mme Frédérique DREIFUSS-NETTER, suppléante ;
Dans le domaine de la sécurité des systèmes d'information et des nouvelles technologies :
M. Henri SERRES, titulaire, et M. Robert PICARD, suppléant ;
Dans le domaine économique et financier :
M. Jean-Claude MOISDON titulaire, et M. Dominique TONNEAU, suppléant.

M. le docteur Philippe BICLET est désigné comme président.

ARRÊTÉ DU 21 FÉVRIER 2006 MODIFIANT L'ARRÊTÉ DU 7 FÉVRIER 2006 FIXANT LA COMPOSITION DU COMITÉ D'AGRÉMENT DES HÉBERGEURS DE DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL

JORF n°49 du 26 février 2006
Texte n°24

ARRETE

Arrêté du 21 février 2006 modifiant l'arrêté du 7 février 2006 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel

NOR: SANC0620689A

« Par arrêté du ministre de la santé et des solidarités en date du 21 février 2006, l'arrêté du 7 février 2006 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel est modifié comme suit :

Au lieu de : « Au titre de personne qualifiée dans le domaine économique et financier
M. Jean-Claude MOISDON, titulaire, et M. Dominique TONNEAU suppléant »,

lire : « Au titre de personne qualifiée dans le domaine économique et financier
M. Jean-Claude MOISDON, titulaire, et M. Olivier LENAY, suppléant ».

ARRÊTÉ DU 15 FÉVRIER 2007 MODIFIANT LES ARRÊTÉS DU 7 FÉVRIER 2006 ET DU 21 FÉVRIER 2006 FIXANT LA COMPOSITION DU COMITÉ D'AGRÉMENT DES HÉBERGEURS DE DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL

JORF n°46 du 23 février 2007
Texte n°76

ARRETE

Arrêté du 15 février 2007 modifiant les arrêtés du 7 et du 21 février 2006 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel

NOR: SANC0720755A

« Par arrêté du ministre de la santé et des solidarités en date du 15 février 2007, les arrêtés du 7 et du 21 février 2006 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel sont modifiés comme suit :

Au lieu de : « Au titre des associations d'usagers compétentes en matière de santé et agréées
MM. Jean-Luc BERNARD et Christian SAOUT, titulaires, et M. Michel DELCEY et Mme Anne LAZARÉVITCH, suppléants »,

Lire : « Au titre des associations d'usagers compétentes en matière de santé et agréées
M. Jean-Luc BERNARD et Mme Anne LAZARÉVITCH, titulaires, et Mme Nadine TELLIER et M. Philippe BERGEROT, suppléants ».

Au lieu de : « Au titre de personne qualifiée dans le domaine de la sécurité des systèmes d'information et des nouvelles technologies:
M. Henri SERRES, titulaire, et M. Robert PICARD suppléant »,

Lire : « Au titre de personne qualifiée dans le domaine de la sécurité des systèmes d'information et des nouvelles technologies
M. Pascal FAURE, titulaire, et M. Robert PICARD, suppléant ».

ARRÊTÉ DU 19 NOVEMBRE 2009 PORTANT MODIFICATION DE L'ARRÊTÉ DU 7 FÉVRIER 2006 FIXANT LA COMPOSITION DU COMITÉ D'AGRÉMENT DES HÉBERGEURS DE DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL

JORF n°0275 du 27 novembre 2009
Texte n°79

ARRETE

Arrêté du 19 novembre 2009 portant modification de l'arrêté du 7 février 2006 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel

NOR: SASG0927586A

« Par arrêté de la ministre de la santé et des sports en date du 19 novembre 2009, l'arrêté du 7 février 2006 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel est modifié comme suit :

Au lieu de : « Au titre de l'inspection générale des affaires sociales
M. Daniel POSTEL-VINAY, titulaire, et M. Christophe LANNELONGUE, suppléant »,

Lire « Au titre de l'inspection générale des affaires sociales
M. Michel DURRAFOURG, titulaire, et M. Thierry LECONTE suppléant ».

Au lieu de : « Au titre des associations d'usagers compétentes en matière de santé et agréées
M. Jean-Luc BERNARD et Mme Anne LAZARÉVITCH titulaires, et Mme Nadine TELLIER et M. Philippe BERGEROT, suppléants »,

Lire : « Au titre des associations d'usagers compétentes en matière de santé et agréées
Mme Nathalie TELLIER et M. Jean-Michel ALCINDOR, titulaires, et MM. René MAZARS et Philippe BERGEROT, suppléants ».

Au lieu de : « Au titre de l'Union nationale des professions de santé
M. le docteur Gérard GALLIOT, titulaire, et M. Patrick CORNE, suppléant »,

Lire : « Au titre de l'Union nationale des professions de santé
M. Patrick CORNE, titulaire, et M. le docteur Gérard GALLIOT, suppléant ».

Au lieu de : « Au titre de personne qualifiée dans les domaines de l'éthique et du droit
M. Gilles BARDOU, titulaire, et Mme Frédérique DREIFUSS-NETTER, suppléante »,

Lire : « Au titre de personne qualifiée dans les domaines de l'éthique et du droit
Mme Isabelle de LAMBERTERIE, titulaire ».

Au lieu de « Au titre de personne qualifiée dans le domaine de la sécurité des systèmes d'information et des nouvelles technologies
M. Pascal FAURE, titulaire, et M. Robert PICARD, suppléant »,

Lire : « Au titre de personne qualifiée dans le domaine de la sécurité des systèmes d'information et des nouvelles technologies
M. Robert PICARD, titulaire ».

ARRÊTÉ DU 14 JUIN 2011 FIXANT LA COMPOSITION DU COMITÉ D'AGRÉMENT DES HÉBERGEURS DE DONNÉES DE SANTÉ A CARACTÈRE PERSONNEL

JORF n°0140 du 18 juin 2011 page 10455
texte n° 39

ARRETE

Arrêté du 14 juin 2011 fixant la composition du comité d'agrément des hébergeurs de données de santé à caractère personnel

NOR: ETSZ1114116A

« Par arrêté du ministre du travail, de l'emploi et de la santé en date du 14 juin 2011, sont nommés pour cinq ans membres du comité d'agrément des hébergeurs de données de santé à caractère personnel :

Au titre de l'inspection générale des affaires sociales

M. Pierre LESTEVEN, titulaire, et M. Jérôme GUEDJ, suppléant.

Au titre des associations compétentes en matière de santé

Mme Nathalie TELLIER et M. Jean-Michel ALCINDOR, titulaires, et M. René MAZARS, suppléant.

Au titre des professions de santé

Sur proposition du Conseil national de l'ordre des médecins :
M. le docteur Jacques LUCAS, titulaire, et M. le docteur Pierre JOUAN, suppléant.
Sur proposition de l'Union nationale des professions de santé :
M. Patrick CORNE, titulaire, et M. le docteur Gérald GALLIOT, suppléant.

Au titre des personnalités qualifiées

En raison de leurs compétences dans les domaines de l'éthique et du droit :
Mme Isabelle de LAMBERTERIE, titulaire, et Mme Anne-Sophie GINON, suppléante ;

En raison de leurs compétences en matière de sécurité des systèmes d'information et de nouvelles technologies :
M. le docteur Philippe BICLET, titulaire, et Mme Martine AUTRAN, suppléante ;

En raison de leurs compétences dans le domaine économique et financier :
M. Robert PICARD, titulaire, et M. Fabrice MATTATIA, suppléant.
M. le docteur Philippe BICLET est désigné comme président. »

ANNEXE 3 : FAQ SUR LE RÉFÉRENTIEL DE CONSTITUTION DES DOSSIERS DE DEMANDE D'AGRÉMENT.

Publié le 08-07-2011 (http://esante.gouv.fr)

Q1 - Quel est le cadre juridique de l'agrément ?

Le cadre législatif de l'activité d'hébergement de données de santé à caractère personnel est fixé par l'article L. 1111-8 du code de la santé publique (loi n° 2002-303 du 4 mars 2002 relative aux droits des patients).

Ces dispositions ont pour objectif d'organiser et d'encadrer le dépôt, la conservation et la restitution des données de santé à caractère personnel, dans des conditions propres à garantir leur confidentialité et leur sécurité.

Le service et les conditions d'hébergement offerts doivent être définis dans un (ou des) contrat(s) établi(s) entre le prestataire hébergeur et les déposants : professionnel ou établissement de santé ou personne concernée par les données.

Pour mémoire, les termes de la loi définissent que *« [...] les hébergeurs tiennent les données de santé à caractère personnel qui ont été déposées auprès d'eux à la disposition de ceux qui les leur ont confiées. Ils ne peuvent les utiliser à d'autres fins. Ils ne peuvent les transmettre à d'autres personnes que les professionnels de santé ou établissements de santé désignés dans le contrat prévu [...] » et que « [...] lorsqu'il est mis fin à l'hébergement, l'hébergeur restitue les données qui lui ont été confiées, sans en garder copie, au professionnel, à l'établissement ou à la personne concernée ayant contracté avec lui. [...] »*

Le décret n°2006-6 du 4 janvier 2006 définit les conditions d'agrément des hébergeurs de données de santé à caractère personnel sur support informatique.

L'agrément est délivré après une évaluation des capacités des candidats, portant sur les aspects financiers, éthiques et de sécurité de leur activité.

Le décret n° 2011-246 du 4 mars 2011 définit les conditions d'agrément des hébergeurs de données de santé à caractère personnel sur support papier. Voir ci-dessous la note sur les conditions d'agrément des hébergeurs de données de santé à caractère personnel sur support papier.

Les questions de la présente FAQ sont relatives à la procédure d'agrément à l'hébergement de données de santé à caractère personnel **sur support informatique**.

Q2 - Quel droit pour les personnes concernées par les données de santé hébergées ?

La loi précise que l'hébergement de données de santé à caractère personnel *« [...] ne peut avoir lieu qu'avec le consentement exprès de la personne concernée. [...] »* notamment lorsque les contractants d'un service d'hébergement sont des professionnels de santé ou des établissements.

Une dérogation à cette obligation a été apportée par l'article 25 de la loi n°2007-117 du 30 janvier 2007, dès lors que l'accès aux données hébergées est limité au seul professionnel de santé ou établissement qui les a déposées, ainsi qu'à la personne concernée ; donc en dehors de toute logique de mise en partage de ces données, le consentement du patient n'est alors plus exigé. Il dispose toutefois, conformément au droit commun issu de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés d'un droit d'opposition et de rectification.

Par ailleurs aucune manipulation des informations de santé, conservées par le prestataire de service d'hébergement, n'est autorisée.

Q3 - La procédure d'agrément s'applique-t-elle aux établissements de santé ?

Les établissements de santé tiennent à jour un dossier hospitalier pour chaque patient pris en charge. Ces dossiers sont conservés pendant 20 ans à compter du dernier séjour du patient dans l'établissement. Ils peuvent être conservés au sein de l'établissement de santé ou confiés à un hébergeur agréé.

Si l'établissement héberge lui-même les dossiers hospitaliers, il n'a pas besoin d'obtenir un agrément. En revanche, si l'établissement met son système d'hébergement au service d'autres établissements de santé, il est soumis à la procédure d'agrément.

Il en est de même pour les établissements de coopération sanitaire (Groupements de coopération sanitaire, Communautés hospitalières …) qui mettent à disposition de leurs membres leur système d'hébergement : ils sont soumis à la procédure d'agrément.

Q4 - Quels sont les apports de l'agrément d'hébergement en termes de confidentialité et de sécurité des données de santé à caractère personnel ?

L'obligation légale pour un promoteur de SIS de faire appel à un hébergeur agréé exonère, de fait, celui-ci d'une grande partie des contrôles vis-à-vis des garanties de confidentialité et de sécurité qui doivent être apportées par son prestataire sur le périmètre exclusif des traitements d'hébergement des données de santé à caractère personnel.

Pour autant, le fait de faire appel à un hébergeur agréé ne le dispense en aucune façon du respect des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés pour ce qui touche à l'ensemble des autres traitements qu'il a prévu de mettre en œuvre dans le cadre de son SIS.

La définition précise, dans le contrat, du périmètre des services entrant dans le champ de l'hébergement est donc essentielle.

Q5 – Une société est-elle agréée pour l'ensemble de ses activités ?

Un candidat peut déposer soit un dossier de demandes d'agrément intégrant autant de types de prestations de service d'hébergement de données de santé qu'il propose sur le marché soit un dossier de demande d'agrément pour chaque type de prestation d'hébergement.

Par types de prestation d'hébergement il faut entendre « modèles de contrats » différents, adaptés à la typologie des clients de l'hébergeur.

Les contrats, mentionnés à l'article R.1111-13 alinéas 2 et 3 du Code de la santé publique, lient le prestataire d'hébergement avec la personne concernée par les données ou un professionnel de santé ou un établissement prenant en charge la personne concernée par les données déposées.

L'agrément est délivré pour un modèle de contrat et non pour l'ensemble des activités de l'hébergeur.

Q6 - Si je lance un appel d'offres pour un système d'information nécessitant un volet hébergement de données de santé à caractère personnel, à quel moment faut-il exiger de mon prestataire de service qu'il soit agréé comme hébergeur ?

Dans le cadre d'un appel d'offre pour un système d'information nécessitant un volet hébergement de données de santé à caractère personnel, si le prestataire n'est pas encore agréé à l'hébergement de données de santé à caractère personnel, il est nécessaire que soit imposée a minima dans l'appel d'offre, une clause imposant au prestataire de déposer une demande d'agrément à l'hébergement de données de santé à caractère personnel.

Q7 – Comment se positionnent les traitements de contrôle d'accès aux données vis-à-vis de la procédure d'agrément ?

Le prestataire de service d'hébergement doit évidemment mettre en œuvre un contrôle d'accès. Toutefois le périmètre du contrôle d'accès entrant dans le champ de la procédure d'agrément se limite à l'authentification de l'identité des personnes déclarées dans le contrat d'hébergement.

Si un promoteur de SIS souhaite mettre en œuvre un contrôle d'accès avec un niveau de granularité plus fin ou des critères différents (spécialités des PS par exemple), ce contrôle d'accès est exclu du champ de l'agrément et doit-être considéré comme un traitement applicatif entrant dans le champ de la loi Informatique et Libertés (même si traitement de contrôle d'accès complémentaire sont assurés par l'hébergeur).

Q8 – L'obligation légale de contractualisation entre un hébergeur agréé et les déposants de données de santé à caractère personnel aura-t-elle un impact sur la situation actuelle vis-à-vis de ses clients ?

Les dispositions de l'article L.1111-8 du code de la santé publique auront inévitablement un impact important sur les contrats existants intégrant des prestations de traitements d'hébergement tels que définis par la loi.

Les opérateurs du secteur de la santé vont devoir prendre en compte cette évolution essentielle du cadre législatif du secteur en élaborant des modèles de contrats conformes à cette nouvelle obligation légale qui impose qu'un hébergeur de données de santé à caractère personnel contractualise avec la personne concernée par les données déposées ou avec un professionnel de santé ou un établissement prenant en charge cette personne.

Ils devront différencier clairement les contrats qui relèvent de l'hébergement de données de santé tel que défini à l'article L.1111-8 de ceux qui relèvent d'autres catégories de traitements. Parmi ces traitements, se trouvent par exemple l'exécution de règles de contrôle d'accès évoluées définies dans le cadre d'un SIS particulier pouvant porter sur des critères complémentaires différents de la seule identité de la personne souhaitant accéder aux données.

Si les niveaux de disponibilité ou de performance ne sont pas intégrés directement dans les exigences du décret n°2006-6 du 4 janvier 2006, en revanche la description des indicateurs qui permettent au contractant de vérifier les niveaux de service réellement offerts en fait partie. C'est donc notamment sur ce type de critères, pour lesquels un engagement clair doit être exprimé par l'opérateur dans le contrat, que se fait la différenciation et la mise en concurrence des offres des hébergeurs agréés.

Q9 – La confidentialité des informations présentes dans les dossiers de demandes d'agrément transmis par les candidats est-elle respectée ?

Le ministère chargé de la santé garantit la confidentialité absolue des formulaires et documents complémentaires constituant les dossiers des demandes d'agrément qu'il réceptionne. Des dispositions adaptées sont mises en œuvre tout au long du processus d'analyse des dossiers par l'ensemble des acteurs impliqués dans cette instruction.

Q10 – Quels sont les sous-traitants devant être déclarés ?

L'hébergeur doit déclarer tous les sous-traitants qui, par les missions qui leur sont dévolues, ont accès aux données de santé à caractère personnel. Le sous-traitant doit apporter un niveau de garantie équivalent à celui de l'hébergeur principal. Ces exigences de confidentialité et de sécurité doivent notamment apparaître dans les clauses des différents contrats que l'hébergeur agréé passe avec ses sous-traitants.

En revanche, il n'est pas nécessaire de déclarer les sous-traitants qui ne participent pas directement à l'activité d'hébergement et ne contribuent pas à la sécurité informatique ou physique des données.

Q11 - A partir de quelle durée de conservation des données de santé à caractère personnel un prestataire de service est-il considéré comme hébergeur ?

L'article 4 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, établit que les dispositions de cette loi « ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises ».

Si on transpose cette exclusion au contexte de l'agrément des hébergeurs de données de santé à caractère personnel, les prestataires qui proposent des services de type réseau de télécommunication, pour lesquels la durée du stockage des informations est limitée à la traversée des équipements actifs des réseaux sans mise en œuvre de traitement de niveau applicatif, ne sont pas considérés comme entrant dans le champ de la procédure.

Q12 – Comment peuvent se répartir les responsabilités de couverture des obligations du décret ?

Un candidat à l'agrément des hébergeurs de données de santé doit couvrir, dans son dossier de demande, toutes les obligations qui sont définies dans le décret.

Pour ce faire, il peut décider de répondre lui-même à l'ensemble des exigences. Il peut également choisir de reporter la couverture de certaines d'entre-elles sur ses clients (par des clauses contractuelles spécifiques dans ses contrats types) ou sur ses sous-traitants (au travers des termes des contrats qu'il passe avec ces derniers). Dans ce dernier cas les clients doivent être informés de l'étendu des responsabilités sous-traitées.

Ainsi la responsabilité du contrôle d'accès aux données de santé peut être dévolue au client, sous réserve que celui-ci soit bien informé de ses obligations en la matière.

L'hébergeur exerce en ce sens un devoir de conseil vis-à-vis du client. S'il ne prend pas la responsabilité de l'ensemble de la prestation d'hébergement, il se doit de conseiller le client sur les procédures internes à mettre en place.

Q13 – Les données de santé doivent-elles nécessairement être hébergées sur le territoire français ?

Le contrat d'hébergement indique le lieu où sont hébergées les données.

Rien ne s'oppose à ce qu'une base de données de santé à caractère personnel soit hébergée en dehors du territoire français., La directive communautaire 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données du Parlement européen et du Conseil établit un cadre de protection des données à caractère personnel équivalent à l'ensemble des pays membres de l'Union européenne. Cette directive a été transposée en France par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le transfert de données de santé à caractère personnel vers un pays tiers à l'Union européenne est en principe interdit, cependant les articles 68 et 69 de la loi du 6 janvier 1978 rendent ce transfert possible au travers de mécanismes permettant de s'assurer du niveau de protection adéquat des données :

- La Commission européenne a reconnu comme présentant un niveau de protection adéquat, les pays suivants : Canada, Suisse, Argentine, territoires de Guernesey, de Jersey et de l'Isle de Man.
- Les Biding Corporate Rules (BCR) ou règles internes d'entreprises : règles adoptées au sein d'un groupe multinational. Les BCR doivent revêtir un caractère contraignant et être respectées par les filiales du groupe.
- Les Clauses Contractuelles Types : ce sont des modèles de clauses contractuelles adoptées par la Commission européenne permettant d'encadrer les transferts de données à caractère personnel.
- Le Safe Harbor : le Safe Harbor concerne les entreprises situées aux Etats-Unis. Le Safe Harbor est un ensemble de principes de protection des données personnelles négociées par les autorités américaines et la Commission européenne en 2001. Les entreprises adhérentes au Safe Harbor doivent se conformer aux exigences de protection des données et assurent ainsi un niveau de protection adéquat.

Q14– Quel est le statut du *« médecin de l'hébergeur »* ?

Une des exigences du décret n° 2006-6 du 4 janvier 2006 dans son article R. 1111-9-6 est la présence d'un médecin dans l'organisation candidate à l'agrément.

Il découle de cette exigence que ce médecin doit être inscrit à l'Ordre des médecins.

Comme cela est le cas pour tous les médecins inscrits à l'Ordre, le contrat de travail liant ce médecin au candidat à l'agrément doit obligatoirement être transmis au Conseil Départemental de l'Ordre des Médecins. Le contrôle des contrats est une mission classique de l'Ordre qui vise à vérifier, notamment, que les médecins ne sacrifient pas l'indépendance de leur jugement. A cet égard, retenir le médecin du travail de la société hébergeur n'apparaît pas opportun.

Ce médecin peut exercer dans un pays tiers où les données sont hébergées, en vertu du principe de reconnaissance des diplômes. Dans cette hypothèse, il doit pouvoir s'exprimer en Français et son contrat, rédigé en langue française doit être transmis avec la demande d'agrément.

Le *« médecin de l'hébergeur* » doit être lié contractuellement avec celui-ci, mais il n'est pas obligatoirement un salarié de l'entreprise. Le contrat peut être un contrat de prestation de service, dès lors qu'il existe des clauses d'interdiction d'exercice d'activités incompatibles : médecin des assurances ou médecin du travail par exemple.

Q15 - Quels sont les organismes qui peuvent être hébergeurs de données à caractère personnel ?

L'hébergement est généralement assuré par des sociétés de services informatiques à même de garantir la confidentialité, la sécurité, l'intégrité et la disponibilité des données de santé qui leurs sont confiées. Exceptionnellement les établissements de santé ou leurs groupements peuvent proposer des solutions d'hébergement, sous réserve qu'ils aient obtenu l'agrément.

En revanche les organismes d'administration générale (collectivités territoriales, CCAS …) n'ont pas vocation à héberger des données de santé à caractère personnel.

Q16 - Quelle distinction peut-on faire entre anonymisation et chiffrement des données de santé ?

L'anonymisation est une technique permettant de faire disparaître d'un document toute référence à la personne concernée par les données (nom, numéro de sécurité sociale, INS, adresse …). L'anonymisation peut être irréversible c'est-à-dire qu'il devient impossible de revenir à l'identité de la personne soit directement, soit indirectement. Le contrôle de la CNIL porte alors sur la technique d'anonymisation retenue. L'anonymisation peut aussi être réversible. Dans ce cas, la base de données reste soumise au contrôle de la CNIL et si elle est hébergée, à la nécessité d'obtenir pour l'hébergeur un agrément au titre du décret du 4 janvier 2006.

Le chiffrement est une technique qui consiste à rendre illisible un document pour celui qui ne détient pas la clef de déchiffrement. Différentes techniques de chiffrement plus ou moins sophistiquées existent. Mais, le chiffrement ne remet pas en cause le statut de la donnée au regard de la loi Informatique et Libertés. En conséquence, une base de données à caractère personnel chiffrées reste soumise au contrôle de la CNIL et si elle est hébergée, à la nécessité pour l'hébergeur d'obtenir un agrément, nonobstant le caractère directement ou indirectement nominatif des données concernées.

Q17 - Les avis du Comité d'agrément sont-ils publics ?

Les avis du Comité d'agrément ne sont pas publics. En effet, le Comité se prononce au regard d'éléments fournis par des entreprises et établissements publics dont le caractère confidentiel doit être préservé. Par ailleurs, les avis du Comité d'agrément, comme les avis de la CNIL, ne lient pas le ministre de la Santé qui prend la décision d'agrément.

En application de la loi du 11 juillet 1979 modifiée, les motifs d'un éventuel refus d'agrément sont communiqués au candidat.

Par ailleurs un candidat peut avoir accès à son dossier, conformément à la loi du 17 juillet 1978 relative à la communication des documents administratifs.

Si les avis du comité d'agrément ne sont pas publics, sa doctrine est diffusée au public, à travers la présente foire aux questions, une note de doctrine et un rapport d'activité qui seront publiés au 4ème trimestre de l'année 2010.

Q18 - En matière d'analyse de risques est-il utile de se référer à la norme 27005 ?

Lors de la concertation qui a précédé la relance de la procédure d'agrément des hébergeurs, les opérateurs du secteur de la santé ont fait savoir qu'ils ne souhaitaient pas se voir imposer par les pouvoirs publics une méthodologie particulière Aucune référence à une norme n'est donc imposée aux candidats.

Cependant, le RGS v1.0 recommande l'utilisation de la méthodologie EBIOS qui est conforme à la norme ISO 27005. Le RGS ne s'applique qu'aux autorités administratives et n'est donc pas opposable aux acteurs du secteur privé concernés par l'agrément des hébergeurs mais constitue une référence utile pour les opérateurs privés.

Si l'utilisation d'une méthodologie respectant la norme ISO 27005 ne garantit pas, à elle seule, que le candidat satisfait aux exigences du décret, cette démarche le place dans de bonnes conditions pour atteindre cet objectif. Le résultat final est fonction de la qualité du travail accompli en appliquant la méthode.

Lien courriel pour nous adresser vos questions : contact-agrement-hebergeurs@sante.gouv.fr [2]

Q19 – Quelles sont les clauses à insérer dans le contrat du médecin hébergeur ?

Vous trouverez ci-dessous dans la liste des documents associés un modèle de contrat de médecin de l'hébergeur, à adapter selon les besoins propres de chaque organisme.

Q20 - Quelles sont les procédures particulières à prévoir lorsque l'hébergement ne porte que sur des données chiffrées par le client ?

Certains hébergeurs exigent que les données leur soient transmises chiffrées par le client. Cette procédure pose un problème quant à la garantie de l'intégrité des données. En effet, le médecin de l'hébergeur doit pouvoir accéder aux données en clair, lorsque c'est nécessaire à l'exercice de sa mission. Pour ce faire deux solutions sont proposées :

- Soit le client fournit à l'hébergeur des clés de déchiffrement
- Soit l'hébergeur fournit lui-même au client la formule de chiffrement ou déchiffrement

Lorsqu'aucune de ces solutions n'est prévue, le contrat d'hébergement doit prévoir que le médecin de l'hébergeur accède aux données de santé en clair sur les serveurs du client.

[1] SIS = Système d'Information de Santé

Q21 - Un professionnel de santé ou un établissement peuvent-ils déposer des données de santé à caractère personnel auprès d'un éditeur de logiciels non agréé ?

a) L'hébergement de données de santé à caractère personnel ne peut être effectué que par un organisme agréé hébergeur au sens de la l'article L 1111-8 du code de la santé publique et du décret 2006-6 du 4 janvier 2006.

b) Si l'éditeur retenu par le professionnel de santé ou l'établissement de santé héberge les données ainsi déposées, il doit satisfaire aux conditions d'agrément prévues part les textes.

Il peut également confier cette prestation d'hébergement d'applications en mode SaaS (ou équivalent) à un organisme tiers agréé hébergeur de données de santé à caractère personnel pour la même famille de service (service en mode SaaS).

Le contrat d'hébergement conclu entre l'éditeur de logiciels et l'hébergeur agréé doit garantir le respect d'obligations énoncées à l'article R 1111-13 du code de la santé publique (article issu du décret 2006-6 du 4 janvier 2006) relatif au contrat d'hébergement et notamment prévoir les modalités de recueil du consentement de la personne concernée par les données de santé hébergées.

Le contrat conclu entre l'éditeur de logiciel et le professionnel de santé ou l'établissement de santé devra notamment mentionner que le logiciel objet du contrat et les données de santé gérées par le logiciel sont hébergés chez un hébergeur agréé ; l'étendue de la prestation pour laquelle l'hébergeur a été agréé, la nécessité de recueillir le consentement de la personne concernée à l'hébergement et les modalités d'accès des professionnels de santé aux données de santé.

Q22 - Puis-je héberger des données de santé à caractère personnel sur une infrastructure de type Cloud computing ?

Rien ne s'oppose à ce que des données de santé à caractère personnel soient hébergées sur une infrastructure de type Cloud computing, à condition que d'une part l'hébergement physique du Cloud computing respecte la réglementation de protection des données de santé à caractère personnel lorsque l'hébergement de telles données a lieu en dehors du territoire français (Voir la question 13) et que d'autre part, l'hébergement au sein de cette infrastructure de type Cloud computing réponde à toutes les exigences sécuritaires du décret hébergeur.

ANNEXE 4 – RÉPONSE DE LA MISSION JURIDIQUE DES AFFAIRES SOCIALES, 10 MAI 2011

Jean-François Mary Le 10 mai 2011

Conseiller d'Etat

Mission juridique des affaires sociales

NOTE

Question : les dispositions de l'article L 1111-8 du CSP dans leur rédaction actuelle qui prévoient un dispositif d'agrément des *« hébergeurs de données de santé »* (personnes physiques ou morales) permettent-elles qu'un agrément soit délivré à une société spécialisée dans la conduite de recherches biomédicales pour le compte d'établissements de soins ou de laboratoires pharmaceutiques ?

Le Conseil constitutionnel a jugé à de nombreuses reprises que la liberté proclamée par l'article 2 de la DDH impliquait le droit au respect de la vie privée et que ce droit requérait que soit exercée une particulière vigilance dans la collecte, la transmission et le traitement de ces données (CC 23 juillet 1999 n° 99-416 DC loi portant création de la couverture maladie universelle).

Ces données font partie des catégories particulières dont la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel prévoit qu'elles ne peuvent être traitées à moins que le droit interne ne prévoie des garanties appropriées.

Les données de santé à caractère personnel, parce qu'elles relèvent de l'intimité de la vie privée, doivent faire l'objet d'une protection particulière, exigée tant par l'article 6 de la convention n° 108 du Conseil de l'Europe que par l'article 8 de la directive européenne du 24 octobre 1995. A cet égard la Commission réaffirme la pertinence de sa recommandation du 4 février 1997 sur le traitement des données de santé à caractère personnel : les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt direct du patient et à des fins de santé publique, dans les conditions définies par la loi.

L'activité de l'hébergeur des données de santé est fixée à l'article L 1111-8 du CSP.

L'article L. 1111-8 énumère en ces termes les obligations des hébergeurs :

« Les hébergeurs tiennent les données de santé à caractère personnel qui ont été déposées auprès d'eux à la disposition de ceux qui les leur ont confiées. Il ne peuvent les utiliser à d'autres fins(...).

Lorsqu'il est mis fin à l'hébergement, l'hébergeur restitue les données qui lui ont été confiées, sans en garder copie, au professionnel, à l'établissement ou à la personne concernée ayant contracté avec lui».

On retrouve, à travers ces formules, deux obligations caractéristiques du dépôt au sens des articles 1915 et suivants du code civil: l'obligation de restitution et l'obligation de non-utilisation de la chose déposée (voir comm. RDSS 2002 p. 695).

Comme le dépositaire du droit civil, l'hébergeur ne peut utiliser les données qui lui ont été confiées. Par suite, ils ne peuvent transmettre les données de santé à caractère personnel qui ont été déposées auprès d'eux *« à d'autres personnes que les professionnels de santé ou établissements de santé désignés dans le contrat prévu au 2^{e} alinéa* » selon les termes du sixième alinéa de l'article L. 1111-8.

La rédaction de cette phrase pourrait laisser penser que, lors de la signature de ce contrat, les parties ont la faculté de convenir d'un commun accord des professionnels de santé ou établissements auxquels l'hébergeur pourra transmettre des données, sans violer le secret professionnel.

En réalité le contrat détermine selon quelles modalités la personne désignera les professionnels de santé auxquels l'hébergeur pourra donner accès ou transmettre des données.

Cette désignation est un acte unilatéral, réservé à la personne concernée.

Après avoir énoncé que « *seuls peuvent accéder aux données ayant fait l'objet d'un hébergement les professionnels de santé ou établissements de santé qui les prennent en charge et qui sont désignées par les personnes concernées»*, l'article L. 1111-8 ajoute que doivent être respectées les dispositions des **articles L 1111-7 et L. 1110-4**.

L'article L. 1110-4 vise « les professionnels de santé » mais aussi tout autre organisme participant à la prévention et aux soins, afin d'étendre à cette catégorie les règles du secret professionnel. Les hébergeurs me semblent faire partie de cette seconde catégorie.

Cet article subordonne par ailleurs l'échange d'informations médicales entre professionnels de santé à la condition que les échanges d'informations doivent avoir pour seule finalité « *d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible* » Par suite, seules en sont destinataires des personnes physiques : « les *professionnels* » de santé ou « *l'équipe de soins d'un établissement de santé* ».

L'article L 1111-7 qui organise le droit d'accès du patient aux informations de santé le concernant ne traite que de celles recueillies au cours du diagnostic, du traitement ou d'une action de prévention et a pour finalité d'organiser les modalités d'exercice du libre choix du malade.

Le rapprochement des articles L. 1110-4, L 1111-7 et L. 1111-8 du CSP me semble amener à l'idée que seuls peuvent accéder aux données ayant fait l'objet d'un hébergement, outre la personne concernée, les professionnels de santé ou l'équipe de soins des établissements de santé qui prennent en charge cette personne.

Cet accès ne peut avoir d'autre objet que d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible.

En résumé, les dispositions de l'article L 1111-8 et des articles réglementaires pris sur ce fondement, en particulier le régime d'agrément, ne me semblent s'appliquer à ni aux bases de données constituées au cours d'une recherche biomédicale par un organisme de recherche, ni à toutes bases de données constituées en vue de cette recherche.

En application de l'article 53 de la loi du 6 janvier 1978 informatique et libertés, les traitements de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé sont soumis aux dispositions de cette loi, à l'exception des articles 23 à 26, 32 et 38.

Cet article 53 ajoute que les traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients ne sont pas soumis aux dispositions du présent chapitre. Il en va de même des traitements permettant d'effectuer des études à partir des données ainsi recueillies si ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif.

Nous avons donc bien deux régimes exclusifs l'un de l'autre, celui de l'hébergement des données de santé au sens de l'article L 1111-8 et celui du traitement des données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, sur le fondement de l'article L 1121-1 et de la loi du 6 janvier 1978.

Les organismes qui veulent conserver des données de santé à des fins de recherche n'ont pas dans l'état des textes à recueillir un agrément sur la base de l'article L 1111-8 qui ne concerne que ceux répondant à la définition donnée par cet article.