Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

15 JUIN 2015

MINISTÈRE DES AFFAIRES SOCIALES, DE LA SANTÉ ET DES DROITS DES FEMMES

SECRÉTARIAT GÉNÉRAL

Délégation à la stratégie
des systèmes d'information de santé
(DSSIS)

484

Paris, le **11 JUIN 2015**

Objet : votre demande d'agrément en tant qu'hébergeur de données de santé à caractère personnel

PJ : avis de la CNIL du 5 mars 2015
avis du CAH du 22 mai 2015

Monsieur le Directeur général,

La société Softway Medical Radiologie a déposé une demande d'agrément le 23 avril 2014 pour une prestation d'hébergement de données de santé à caractère personnel collectées au moyen du progiciel « One manager ».

J'ai l'honneur de vous faire part de la décision favorable de la ministre des affaires sociales, de la santé et des droits des femmes qui sera publiée au bulletin officiel du ministère.

Vous trouverez ci-joint, l'avis du comité d'agrément des hébergeurs, assorti de recommandations, ainsi que l'avis de la commission nationale de l'informatique et des libertés.

Je vous rappelle que cet agrément en qualité d'hébergeur de données de santé à caractère personnel est valable pour une durée de trois ans et que vous vous engagez à informer sans délai la ministre chargée de la santé de tout changement concernant les informations communiquées et de toute interruption, temporaire ou définitive, de votre activité d'hébergement.

Des contrôles diligentés par la commission nationale de l'informatique et des libertés ou par l'inspection générale des affaires sociales pourront être conduits pour s'assurer du respect des conditions de l'agrément.

Les services de l'ASIP Santé se tiennent à votre disposition pour vous fournir toutes informations complémentaires.

Je vous prie d'agréer, Monsieur le Directeur général, l'expression de ma considération distinguée.

Le délégué

Philippe BURNEL

Monsieur Franck ROBERT
Directeur général Opérationnel
Softway Medical Radiologie
Route de la côte d'Azur Arteparc –Bât C
Rue de la Belle du Canet – CS 20011
13590 MEYREUIL

RÉPUBLIQUE FRANÇAISE

Ministère des affaires sociales,
de la santé et des droits des femmes

Décision du 11 JUIN 2015

portant agrément de la société Softway Medical Radiologie
pour une prestation d'hébergement de données de santé à caractère personnel collectées au moyen du progiciel « One manager ».

NOR

La ministre des affaires sociales, de la santé et des droits des femmes

Vu le code de la santé publique, et notamment ses articles L.1111-8 et R.1111-9 à R.1111-15-1 ;

Vu l'avis de la commission nationale de l'informatique et des libertés en date du 5 mars 2015 ;

Vu l'avis du comité d'agrément des hébergeurs de données de santé à caractère personnel en date du 22 mai 2015.

Décide

Article 1er :

La société Softway Medical Radiologie est agréée en qualité d'hébergeur de données de santé à caractère personnel pour une prestation d'hébergement de données de santé à caractère personnel collectées au moyen du progiciel « One manager ».

Article 2 :

La société Softway Medical Radiologie s'engage à informer sans délai la ministre chargée de la santé de tout changement affectant les informations communiquées et de toute interruption, temporaire ou définitive, de son activité d'hébergement.

Article 3 :

Le délégué à la stratégie des systèmes d'information de santé est chargé de l'exécution de cette décision qui sera publiée au bulletin officiel du ministère des affaires sociales, de la santé et des droits des femmes.

Fait le 11 JUIN 2015

Pour la ministre et par délégation
Le délégué
Philippe BURNEL

Avis du Comité d'agrément des hébergeurs du 22 mai 2015

Vu le code de la santé publique, et notamment ses articles L. 1111-8 et R.1111-9 à R.1111-15-1 ;
Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 5 mars 2015;
Vu l'arrêté du 14 juin 2011, modifié fixant la composition du Comité d'agrément des hébergeurs de données de santé à caractère personnel.

Le comité d'agrément des hébergeurs propose l'agrément pour une durée de trois ans de la société Softway Medical Radiologie pour une prestation d'hébergement de données de santé à caractère personnel collectées au moyen du progiciel « One manager ».

Le comité d'agrément des hébergeurs assortit cette proposition des recommandations suivantes.

- La convention conclue entre le candidat, Softway Medical Radiologie, et le sous-traitant, Softway Medical Infrastructure, doit préciser les prestations réalisées par ce dernier dans le cadre du service d'hébergement de données de santé.

- La nouvelle rédaction de l'article 3 du contrat d'hébergement doit être revue afin de préciser la notion de « titulaire du traitement ».

- Le candidat doit présenter un plan de reprise d'activité à l'état de l'art.

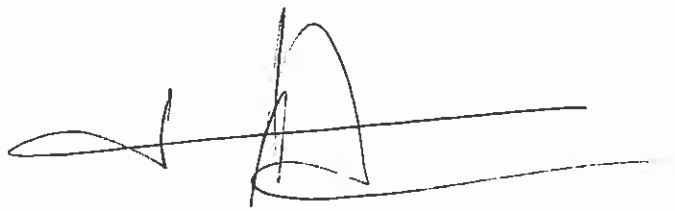
- Le candidat doit décrire les mécanismes d'accès aux traces sauvegardées et aux traces archivées.

- Le candidat doit formaliser une classification et une gestion des incidents permettant de garantir que toute divulgation ou altération de données de santé entraîne la mise en place de la cellule de crise.

- Le candidat doit utiliser un algorithme de chiffrement à l'état de l'art pour les fichiers de sauvegarde.

- Le programme d'audit référencé dans le dossier doit être communiqué.

- La gestion des évolutions des formats des données de santé doit être prise en compte.



Docteur Philippe Biclet, Président du Comité d'agrément des hébergeurs

CNIL.

Délibération n° 2015-082 du 5 mars 2015 portant avis sur la demande d'agrément présentée par la société Softway Medical Radiologie, candidate à l'hébergement de données de santé à caractère personnel

(Saisine n° 14027397)

La Commission nationale de l'informatique et des libertés,

Saisie pour avis par le ministère des affaires sociales, de la santé et des droits des femmes du dossier de demande d'agrément de la société Softway Medical Radiologie, candidate à l'hébergement de données de santé à caractère personnel ;

Vu la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu le code de la santé publique, notamment ses articles L. 1110-4, L. 1111-8 et R. 1111-1 à R. 1111-15-1 ;

Vu le code de la sécurité sociale, notamment son article L. 161-36-1 ;

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

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié, pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le dossier et ses compléments ;

Sur la proposition de M. Alexandre LINDEN, commissaire, et après avoir entendu les observations de M. Jean-Alexandre SILVY, commissaire du Gouvernement ;

Formule les observations suivantes :

La Commission nationale de l'informatique et des libertés est saisie pour avis par le ministère des affaires sociales, de la santé et des droits des femmes, conformément aux dispositions de l'article R. 1111-10 du code de la santé publique, de la demande d'agrément présentée par la société Softway Medical Radiologie, candidate à l'hébergement de données de santé à caractère personnel.

La Commission doit se prononcer, conformément auxdites dispositions, sur « *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 rappelle que quel qu'ait été son avis, émis au vu du dossier qui lui a été communiqué, elle a le pouvoir de diligenter des contrôles auprès de tout responsable de traitement afin de procéder à toute opération de vérification nécessaire, conformément aux dispositions des articles 44 de la loi du 6 janvier 1978 modifiée et 57 et suivants du décret n° 2005-1309 du 20 octobre 2005 pris pour application de cette loi.

Emet dans ces conditions l'avis suivant :

Candidat hébergeur	Softway Medical Radiologie, société par actions simplifiée immatriculée au registre du commerce et des sociétés d'Aix-en-Provence sous le numéro 342 504 297, est une filiale du groupe Softway Medical spécialisée dans l'édition et l'intégration de logiciels pour les cabinets de radiologie et les établissements de santé.
Services proposés	L'hébergeur propose une prestation d'hébergement de données de santé accompagnée du logiciel de gestion des données dénommé « One Manager ». Cette offre est destinée aux établissements de santé et aux cabinets de radiologie. Les clients de l'hébergeur peuvent également faire héberger par la société Softway Medical Radiologie d'autres applicatifs qu'ils fournissent eux-mêmes. La prestation d'hébergement repose sur deux sites physiques appartenant à des sous-traitants : un site principal chez la société Télécity Group et un site de secours chez la société Interxion.
Information et consentement du patient	Le modèle de contrat fourni par l'hébergeur, composé du bulletin de souscription, des conditions générales et des conditions particulières, prévoit un report sur les clients de la responsabilité d'informer les patients et de recueillir leur consentement à l'hébergement des données qui les concernent. La Commission relève que l'hébergeur ne fournit pas à ses clients de modèle de formulaire d'information et de recueil du consentement. Afin qu'il s'acquitte véritablement de son devoir de

	conseil à l'égard de ses clients, la Commission demande que le modèle de contrat soit complété sur ce point.
Exercice du droit d'accès par le patient	L'hébergeur reporte sur ses clients la responsabilité et l'organisation de l'accès des patients aux données de santé qui les concernent par des clauses contractuelles spécifiques qui figurent dans le modèle de contrat fourni par l'hébergeur. La Commission relève que l'hébergeur informe ses clients qu'un contrôle des accès et des règles de sécurité doit être mis en œuvre pour encadrer l'exercice du droit d'accès par le patient. Elle estime que, ce faisant, l'hébergeur satisfait à son devoir de conseil envers ses clients sur ce point.
Politique de contrôle d'accès	**Etablissements et professionnels de santé** La gestion de la politique d'habilitation des professionnels de santé est reportée contractuellement sur les clients de l'hébergeur. Aux termes des conditions générales de l'hébergeur, l'applicatif fourni par ce dernier comporte une interface permettant de gérer les comptes d'utilisateurs, et notamment de leur fournir un mot de passe pour l'accès au logiciel. Bien que les conditions particulières du service rappellent aux clients de l'hébergeur que l'authentification des professionnels de santé doit être opérée par le recours à une carte de professionnel de santé (CPS), la Commission demande que les conditions générales soient modifiées, conformément aux dispositions de l'article L. 1110-4 du code de la santé publique, en imposant un système d'authentification forte des professionnels de santé par l'utilisation d'une CPS ou d'un dispositif équivalent agréé par l'organisme chargé d'émettre la CPS pour toute transmission ou tout accès aux données de santé.
	Personnes concernées par les données (patients) Sans préjudice du droit d'accès direct qui peut être exercé auprès de ses clients, l'hébergeur n'offre pas d'accès informatique direct des patients aux données les concernant.
	Personnel de l'hébergeur L'hébergeur a mis en place une gestion des habilitations en fonction du rôle des intervenants. Une revue de ces habilitations est opérée quotidiennement, afin de révoquer les comptes inactifs depuis quatre mois. Les comptes révoqués sont automatiquement supprimés après un nouveau délai de trois mois si le compte n'a

	pas fait l'objet d'une demande de réactivation. Chaque utilisateur dispose d'un identifiant qui lui est propre. Le personnel de l'hébergeur s'authentifie sur le réseau de l'hébergeur au moyen d'un dispositif d'authentification forte, nécessitant l'utilisation d'un certificat électronique. De plus, l'accès aux ressources des serveurs nécessite une nouvelle authentification soit par l'utilisation d'un certificat RSA pour les administrateurs qui disposent de privilèges élevés sur le système, soit par l'utilisation d'un identifiant et d'un mot de passe dont la complexité est conforme aux recommandations de la Commission pour les autres personnels.
Traçabilité des actions des professionnels de santé	La politique de traçabilité des actions sur l'applicatif fourni par l'hébergeur n'est pas clairement explicitée dans le dossier fourni par ce dernier. Ainsi, sans distinction selon la solution logicielle utilisée par les clients de l'hébergeur, ce dernier « *met en place des dispositifs de contrôle des droits d'accès aux équipements et de traçabilité des accès aux mêmes équipements et procède à des vérifications régulières des logs afin de détecter les tentatives d'accès non autorisées* ». Dès lors que l'hébergeur fournit l'applicatif de gestion des données de santé, la Commission estime qu'il devrait prévoir et décrire dans son dossier de demande d'agrément les modalités de conservation des traces des actions des professionnels de santé, ainsi que la mise à disposition de ces traces aux clients. Dans l'hypothèse où l'hébergeur ne fournit pas l'applicatif de gestion des données de santé, l'annexe intitulée « politique de gestion des accès » précise que l'hébergeur n'est pas en mesure d'assurer la traçabilité des actions réalisées par les professionnels de santé et que cette obligation repose sur ses clients. La Commission en prend acte mais demande que le modèle de contrat soit précisé afin que les responsabilités des parties en matière de traçabilité des actions soient clairement réparties.
Sécurité des données (chiffrement des données chez l'hébergeur et confidentialité	La Commission relève que les transferts de données sont sécurisés par le recours à des réseaux virtuels privés utilisant l'algorithme de chiffrement 3DES. Elle recommande de recourir à l'algorithme AES.

des transmissions)	Elle rappelle que les autres flux de données, notamment ceux existant entre les sites d'hébergement, doivent également être sécurisés en utilisant des protocoles conformes à l'état de l'art, afin de garantir la confidentialité et l'intégrité des données qui y transitent. Seules les sauvegardes destinées à être conservées hors des locaux de l'hébergeur sont chiffrées. La Commission demande que les sauvegardes de données, y compris celles conservées dans les locaux de l'hébergeur, soient chiffrées afin d'en assurer la confidentialité, notamment en cas de vol des supports de conservation des données. La Commission relève que l'hébergeur dispose d'une « politique d'usage de la cryptographie » qui lui permet de vérifier la robustesse des algorithmes de chiffrement ou de hachage qu'il utilise.
Pérennité des données	Conformément aux modalités de réponse à l'obligation de sécurité suggérées dans les recommandations de la CNIL sur le cloud computing, qui ont été rendues publiques le 25 juin 2012, le candidat à l'agrément doit s'assurer de la disponibilité et de la pérennité des données. L'hébergeur assure une gestion des services critiques de nature à assurer l'intégrité du matériel hébergé. L'hébergeur dispose de deux sites physiques distants sur lesquels les données sont répliquées au fil de l'eau. Il sauvegarde les données quotidiennement sur le site de secours et sur le site principal. Les sauvegardes dont la durée de rétention est supérieure à deux mois sont externalisées dans le coffre-fort d'une banque. Des tests de restauration des sauvegardes sont réalisés tous les six mois afin de vérifier le bon fonctionnement de celles-ci. La Commission relève que l'hébergeur vérifie que les empreintes MD5 des fichiers, générées lors de leur sauvegarde, et lors de la restauration, sont identiques pour vérifier que ces fichiers n'ont pas été modifiés, alors que l'algorithme MD5 n'est pas considéré comme fiable pour s'assurer de l'intégrité des fichiers. La Commission demande que les empreintes des fichiers soient réalisées avec un autre algorithme tel que l'algorithme SHA-256.
Observations propres au	La Commission recommande que l'hébergeur transmette à son

traitement	client les rapports d'auto-évaluation annuels ainsi que les rapports d'audit externe, réalisés en cas de demande de renouvellement de l'agrément.

La Présidente

I. FALQUE-PIERROTIN

Marie-France MAZARS
Vice-président délégué