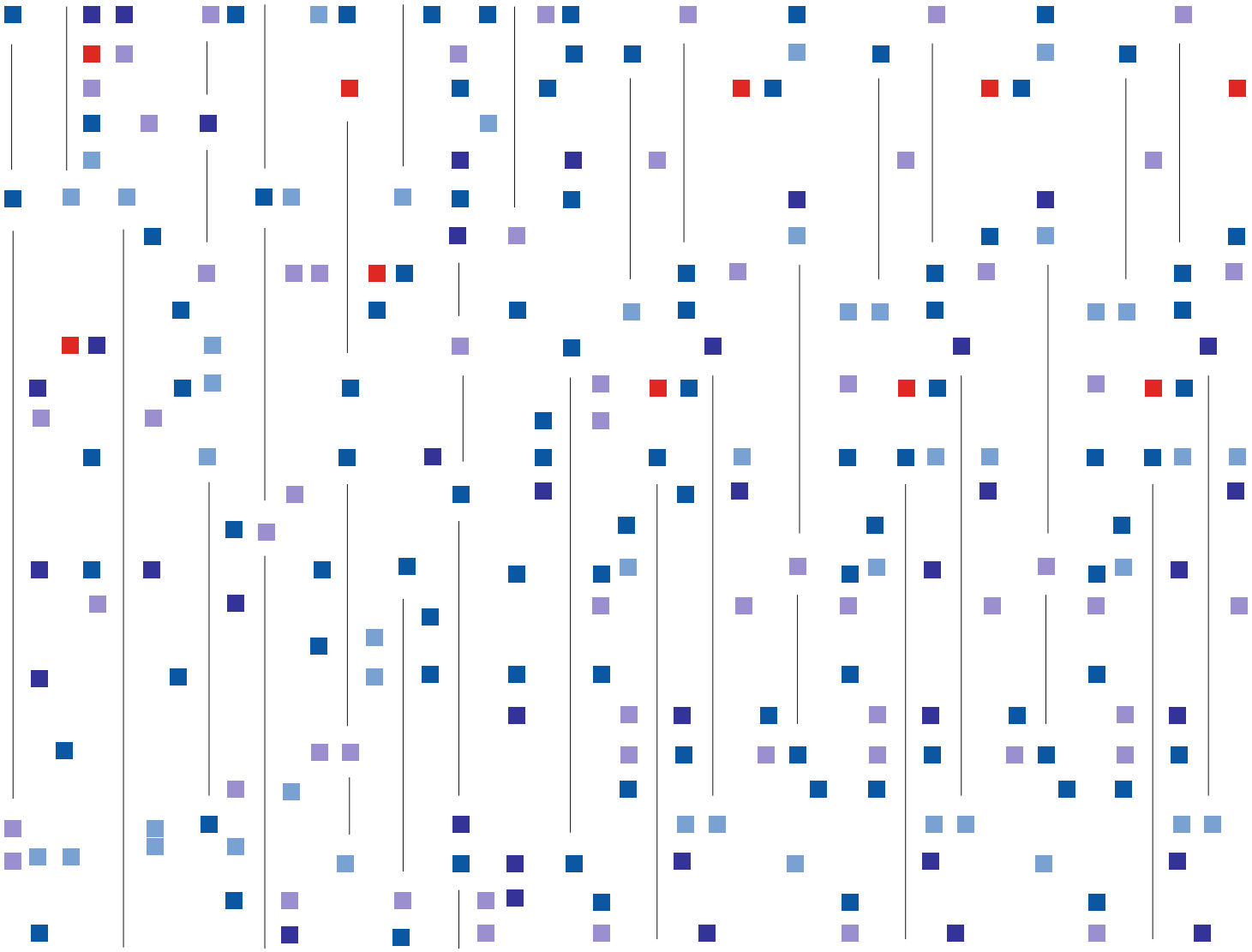
COMITÉ D'AGRÉMENT
DES HÉBERGEURS
DE DONNÉES DE SANTÉ

RAPPORT D'ACTIVITÉ 2012-2013



SOMMAIRE

LE MOT DU PRÉSIDENT

Le deuxième rapport du Comité d'agrément des hébergeurs (CAH), établi au terme de l'instruction de plus de 170 dossiers, reflète désormais l'âge adulte de la procédure.

Le CAH, bien conscient des complications administratives et des complexités techniques, a tenté, en bonne intelligence avec la seconde instance de régulation qui participe à la procédure, la CNIL, et l'opérateur central des systèmes d'information, l'ASIP Santé, d'apporter sa vision pragmatique.

Cette politique, reflet d'une large collégialité éthique, juridique et technique a été reconnue par tous les acteurs.

D'autres étapes sont devant nous afin, tout à la fois, d'augmenter les garanties et de fluidifier les procédures.

Le périmètre de l'hébergement agréé ne peut être fixé dans les tables, il doit évoluer avec la vie des professions, les développements technologiques. Une réflexion forte et urgente doit, par exemple, se mettre en place sur les bases détenues par les assureurs privés et publics.

Le décret du 4 janvier 2006 fixant les règles de l'hébergement doit être aménagé afin d'assurer à la fois plus de convergence et de complémentarité entre les expertises menées par la CNIL et le comité d'instruction placé auprès du CAH.

L'analyse économique et financière, gage de pérennité des données qui ne peuvent être confiées à des structures fragiles reste justifiée, mais elle doit être repensée pour prendre en compte la vie financière réelle des industriels : que signifie le bilan financier déficitaire d'un hôpital public qui sera nécessairement contraint d'exécuter ses missions de service public ? Quel est l'intérêt et où trouver les compétences pour procéder à l'expertise de la comptabilité d'une société cotée au Nasdaq, dont la filiale française demande l'agrément et dont la société mère peut désirer se défaire ?

Enfin, il faudra améliorer de manière exigeante autant que réaliste les procédures d'audit. C'est d'ailleurs une démarche à engager de concert avec les acteurs responsables de la profession bien conscients des enjeux sociétaux.

Le Comité est convaincu du rôle essentiel que la procédure d'agrément a rempli pour élever les niveaux de sécurité et de responsabilisation des industriels et leur permettre d'accroître la confiance des usagers. C'est dans cette direction qu'il faut continuer pour faire évoluer les comportements des professionnels et des patients dans un but commun : le juste soin.

DR PHILIPPE BICLET,
président du Comité d'agrément des hébergeurs

LE RÔLE DES HÉBERGEURS DE DEMAIN

Demain, l'obligation pour les organismes qui souhaitent héberger des données de santé à caractère personnel de voir leurs capacités évaluées au regard d'un ou plusieurs référentiels sera devenue aussi habituelle que le respect des normes de sécurité physique.

Demain, les hébergeurs auront un rôle d'éducation des individus à l'égard du traitement de leurs données personnelles. Ils devront faire de la pédagogie autour de leur métier et assurer une représentation des patients au sein de leur conseil d'administration.

Demain, les hébergeurs consacreront une partie de leurs revenus obtenus à partir de l'hébergement à la pédagogie et à rendre publiques des études effectuées à partir des données hébergées dans le respect des règles de protection des données.

Demain, les hébergeurs rendront publics auprès des personnes dont ils hébergent les données, les résultats des audits effectués et permettront aux personnes concernées un accès direct et dématérialisé à leurs données hébergées.

Mais demain se prépare aujourd'hui…

Le Dr Richard Fitton travaille pour le National Health Service (NHS), le système de santé publique du Royaume-Uni. Il est reconnu, tant au niveau national qu'international, comme l'un des principaux défenseurs d'un contrôle accru par les patients de leurs données de santé.

Le Comité d'agrément des hébergeurs **(CAH)**, organe consultatif créé par le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel, a analysé ses premiers dossiers de demande d'agrément pour l'hébergement de données de santé dès la nomination de ses membres par arrêté du ministre en charge de la santé du 7 février 2006, modifié.

Depuis la reprise de la procédure d'agrément (dont la gestion a été confiée à l'Agence des systèmes d'information partagés de santé ASIP Santé – lors de sa création en 2009) après une suspension décidée par les pouvoirs publics pendant deux ans, le CAH a vu son activité s'accroître et a ainsi analysé 170 dossiers de demande d'agrément.

Cette procédure a été initialement voulue par le législateur, puis a été mise en œuvre par les pouvoirs publics pour sécuriser l'externalisation des bases de données de santé à caractère personnel. Elle vise à assurer le citoyen que ses propres données de santé sont correctement conservées et peuvent lui être restituées quand il le souhaite, sans dégradation ni problème de sécurité et dans le respect de ses droits. Cette procédure n'est pas qu'administrative. Elle vise également à amener les hébergeurs vers un état de l'art qui évolue nécessairement avec le temps. En outre, les capacités techniques d'hébergement se modifient et les solutions informatiques qui peuvent y répondre également.

La technique a changé et sur ce point, les hébergeurs en sont eux-mêmes les instigateurs en développant de nouvelles offres avec le *cloud computing*, des solutions de mobilité, etc.
Outre les évolutions technologiques, le droit a également évolué. Citons à titre d'exemple la prise en compte des dispositions introduites par la loi « Hôpital Patients Santé Territoires » (HPST) du 21 juillet 2009 s'agissant de l'utilisation de dispositifs d'authentification équivalant à la carte de professionnel de santé (CPS) ou encore des référentiels de sécurité et d'interopérabilité mentionnés dans la loi. Il convient également de prendre en compte les travaux menés par l'ASIP Santé et coordonnés par la Délégation à la stratégie des systèmes d'information de santé (DSSIS), dans le cadre de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S), qui associent l'ensemble des acteurs concernés (CNIL, ANSSI, CNAMTS, fédérations d'industriels, représentants d'ordres des professions de santé…), qui sont susceptibles d'impacter l'appréciation qui peut être faite des mesures de sécurité mises en œuvre par les hébergeurs. La procédure d'agrément est ainsi une procédure évolutive. Cela a pour conséquence que les services d'hébergement de données de santé à caractère personnel agréés en 2009 pourraient ne pas l'être trois ans après. Toutefois, la nécessité de déposer un dossier de demande de renouvellement tous les trois ans permet de maintenir un niveau de sécurité à l'état de l'art, commun à tous les hébergeurs agréés.

La procédure d'agrément fait intervenir différents collèges. La Commission nationale de l'informatique et des libertés (CNIL) et le CAH ont, comme toute collégialité composée de personnalités aux compétences et origines professionnelles différentes, des appréciations qui leur sont propres. C'est à cette appréciation qu'il faut attribuer le fait qu'il a été décidé de surseoir à statuer sur certains dossiers de demande d'agrément, alors qu'une lecture automatique du texte aurait conduit à les rejeter.
Le CAH a également pu constater et s'en est ému, que de nombreux dossiers de demande d'agrément reçus manquaient de rigueur. Il l'a alors signalé aux candidats concernés, en rappelant que l'hébergement de données de santé à caractère personnel est une activité exigeante qui implique qu'on s'y engage avec les moyens appropriés.
Même si l'on peut distinguer des éléments essentiels, sans lesquels aucun agrément n'est possible et d'autres plus accessoires, une demande de renouvellement d'agrément qui, par exemple, ne comporterait toujours pas le contrat avec le médecin de l'hébergeur demandé lors de l'agrément initial conduit logiquement à s'interroger sur l'approche qualité de l'hébergeur agréé.

Dès lors, l'appréciation des dossiers de demande d'agrément est réalisée au regard d'un texte, d'un état de l'art qui évolue et d'une appréciation collégiale.

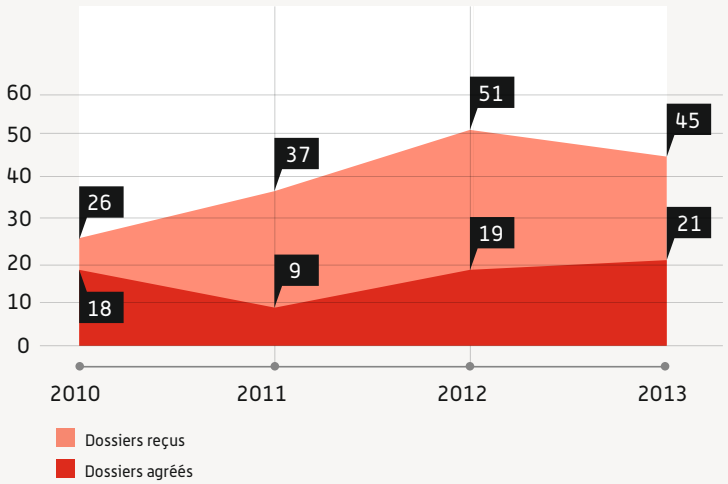
Dans le cadre de ce deuxième rapport d'activité, qui couvre les années 2012 et 2013, le CAH souhaite présenter un bilan chiffré des dossiers analysés, dresser un état des lieux des grands axes d'analyse des dossiers et apporter de nouveaux éléments de doctrine.

CAH

Le Comité d'agrément des hébergeurs est un organe consultatif créé par le décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel, chargé d'émettre un avis sur les dossiers de demande d'agrément, après celui délivré par la CNIL. Les avis de la CNIL et du CAH sont ensuite transmis au ministre en charge de la santé qui décide ou non d'agréer le candidat.

L'activité du CAH en quelques chiffres

Depuis 2009, le secrétariat du CAH a reçu 178 dossiers de demande d'agrément, dont 96 entre 2012 et 2013.
Sur la période 2012-2013, 24 séances du CAH se sont tenues, à fréquence d'une réunion par mois, et un peu plus de 70 dossiers de demande d'agrément ont été analysés par le Comité.



La nécessité de recourir à un hébergeur agréé pour l'hébergement de données de santé a rencontré l'adhésion des structures de soins et professionnels de santé dès lors qu'ils externalisent des données de santé à caractère personnel. Cela a pour effet une activité riche et soutenue du Comité d'agrément. Dans le cadre de l'analyse de ces nombreux dossiers, le CAH veille à ce que son instruction reste fidèle à l'esprit de cet agrément qui a pour finalité la protection des données de santé.

L'activité du CAH a notamment été marquée en 2012-2013 par l'analyse d'un nouveau type de dossier de demande d'agrément : les dossiers de demande de renouvellement d'agrément. Ces dossiers ont suscité de nombreuses questions de la part des candidats au renouvellement, mais aussi des différentes instances qui participent à la procédure d'agrément.

01

Les dossiers de demande de renouvellement d'agrément

Sur la période 2012-2013, le CAH a reçu les premiers dossiers de demande de renouvellement d'agrément. Seize dossiers ont été reçus : douze agréments ont ainsi été renouvelés et quatre demandes sont en cours d'instruction *(chiffres de février 2014)*.

L'ESSENTIEL

Ce que doit renseigner l'hébergeur dans son dossier de demande de renouvellement d'agrément

L'hébergeur doit utiliser le formulaire de constitution de dossier de demande de renouvellement d'agrément disponible sur le site de l'ASIP Santé * et ainsi renseigner les points suivants.

* http://esante.gouv.fr/services

■ **Prise en compte des recommandations** qui accompagnaient la décision d'agrément initial.

■ **Présentation des modifications apportées au service d'hébergement** (dues à l'évolution du cadre juridique, de l'état de l'art et des doctrines de la CNIL et du CAH et modifications souhaitées par l'hébergeur pour améliorer son service).

■ **Rapport d'audit externe de sécurité**.

■ **Informations comptables.**

Les conditions de renouvellement d'agrément sont définies par l'article R.1111-15 du code de la santé publique, qui dispose que *« l'agrément est délivré aux hébergeurs de données de santé à caractère personnel sur support informatique 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 œuvre 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 ».*

L'hébergeur doit donc déposer un dossier de demande de renouvellement comprenant les informations suivantes.

■ Les éléments financiers visés au 8° de l'article R.1111-12, à savoir:

— un document présentant les comptes prévisionnels de l'activité d'hébergement ;
— les comptes de résultat et bilans liés à l'activité d'hébergement depuis le dernier agrément ;
— éventuellement, les trois derniers bilans et la composition de l'actionnariat de l'hébergeur.

■ Les modifications intervenues depuis l'agrément initial sur les autres points de l'article R.1111-12, reproduits ci-dessous:

— éléments relatifs à l'identification de l'hébergeur (nom, adresse), à ses statuts ;
— informations des opérateurs en charge du service d'hébergement de données de santé ;
— lieux d'hébergement ;
— présentation du service d'hébergement ;
— contrat d'hébergement ;
— dispositions mises en œuvre pour garantir la disponibilité, l'intégrité, la confidentialité et l'audibilité des données de santé ;
— recours à des prestataires techniques externes.

■ Un audit externe réalisé aux frais de l'hébergeur attestant de la mise en œuvre de la politique de confidentialité et de sécurité mentionnée à l'article R.1111-14 du code de la santé publique.

Les premiers dossiers de renouvellement ont, dès leur réception, montré une très grande hétérogénéité dans leur présentation : certains étaient présentés sous la forme d'une simple lettre, d'autres s'avéraient immédiatement incomplets.

Il est ainsi rapidement apparu, tant sur le plan juridique que technique, que ces dossiers ne répondaient pas aux exigences posées par le texte.

Face aux enjeux industriels que représentent ces hébergements et soucieux de préserver les données sensibles ainsi confiées aux hébergeurs, la décision a été prise en Comité d'agrément de surseoir à statuer sur ces demandes plutôt que de risquer d'émettre des avis défavorables sur les dossiers.

Un courrier a donc été adressé à chaque hébergeur pour lui rappeler les exigences du texte et la nécessaire prise en compte des recommandations émises par le ministre en charge de la santé au moment de l'agrément initial.

Afin d'accompagner les hébergeurs agréés à constituer leurs dossiers de demande de renouvellement d'agrément et les orienter sur le contenu de l'audit externe de sécurité exigé par les textes, un formulaire de dossier de demande de renouvellement a été publié sur le site esante.gouv.fr.

La publication de ce formulaire a fortement aidé les hébergeurs et le CAH a ainsi pu noter que les dossiers reçus étaient complets.

En outre, une réunion organisée par l'ASIP Santé en accord avec le CAH, le 13 septembre 2013, réunissant la communauté des hébergeurs, a également permis de rappeler la procédure et ses exigences et d'entendre les questions des hébergeurs.

Le CAH a ainsi défini trois axes d'analyse des dossiers de demande de renouvellement.

A – LA PRISE EN COMPTE DES RECOMMANDATIONS ÉMISES PAR LE MINISTRE EN CHARGE DE LA SANTÉ

Les agréments sont délivrés avec des recommandations qui sont des points d'attention relevés lors de l'analyse du dossier de demande d'agrément, mais qui, au regard de la situation de l'hébergeur, du contexte du dépôt du dossier de demande d'agrément et du périmètre de la prestation agréée, n'ont pas été considérées, au moment de l'agrément initial, comme des éléments de nature à entraîner un refus d'agrément.

Jusqu'en 2013, ces recommandations étaient précisées dans le courrier de notification d'agrément qui accompagne la décision d'agrément. **Depuis mi-2013, le courrier de notification d'agrément du ministre en charge de la santé renvoie aux recommandations de la CNIL et du CAH et annexe à cet effet ces deux avis.**

Ces recommandations doivent être prises en compte par l'hébergeur afin d'améliorer son service d'hébergement de données de santé à caractère personnel.

Lors de l'analyse des dossiers, la CNIL et le CAH vérifient que l'hébergeur a bien pris en compte ces recommandations. En effet, cette première

étape permet d'apprécier si l'hébergeur s'inscrit dans une perspective d'amélioration continue de son service d'hébergement.
L'absence de prise en compte des recommandations qui accompagnent la décision d'agrément conduit le CAH à s'interroger sur le « processus qualité » de l'hébergeur et son intérêt à adapter son service à l'ensemble des spécificités de l'hébergement de données de santé à caractère personnel.

B – LES MODIFICATIONS APPORTÉES AU SERVICE D'HÉBERGEMENT DE DONNÉES DE SANTÉ AGRÉÉ

Le dossier de demande de renouvellement d'agrément doit présenter toutes les modifications apportées au dossier de demande d'agrément initial.

Deux grandes catégories d'évolutions peuvent être distinguées.

LES PREMIÈRES SONT MISES EN ŒUVRE PAR L'HÉBERGEUR POUR AMÉLIORER SON SERVICE, MIEUX S'ADAPTER AUX BESOINS DE SES CLIENTS ET AUX EXIGENCES DU MARCHÉ

Ce n'est qu'une fois le service d'hébergement de données de santé réellement proposé, que l'hébergeur va pouvoir évaluer son service au regard des besoins de ses clients et aux exigences du marché.

Exemple d'amélioration en vue de s'adapter aux besoins des clients

■ Un hébergeur agréé pour une prestation d'hébergement de données de santé à caractère personnel, collectées au moyen d'applications fournies par les clients et installées sur l'infrastructure technique de l'hébergeur, réalisait les sauvegardes des données de ses clients sur disques. Au cours de son agrément, l'hébergeur a souhaité modifier sa politique de sauvegarde afin de réaliser des sauvegardes sur bande, qui étaient ensuite chiffrées et externalisées sur un site distant.

■ Un hébergeur agréé pour une « prestation générique » proposait à ses clients des niveaux de services très élevés qui étaient orientés pour répondre aux obligations de continuité d'activité des établissements de santé. En effet, dès lors que l'hébergeur dépose un dossier de demande d'agrément pour une prestation générique, il est tenu de prendre en compte des engagements permettant de répondre aux obligations de tous ses clients potentiels. L'hébergeur a eu comme client un médecin libéral qui exerçait à son cabinet du lundi au vendredi de 9 heures à 18 heures et n'avait donc pas besoin d'un support en 24/7 et d'une garantie de temps de rétablissement du service, y compris la nuit, le week-end et les jours fériés. Ces niveaux de service ont un impact sur le coût de la prestation. L'hébergeur a donc prévu différents niveaux de services, sous réserve d'accompagner le client sur le choix du niveau de service qui lui permettra de répondre à ses obligations.

■ Pour des raisons marketing, certains hébergeurs font également évoluer le nom du service qu'ils proposent, par exemple en introduisant la notion de *cloud computing*.

Ces évolutions ne doivent toutefois pas remettre en cause la sécurité du service, le respect des droits des patients et ne peuvent modifier substantiellement le périmètre du service initialement agréé.

Exemples d'évolutions qui modifient le périmètre de la prestation initialement agréée et exigent le dépôt d'un nouveau dossier de demande d'agrément (et non d'un renouvellement).

■ L'hébergeur est agréé pour un service où il infogère l'ensemble du système, mais souhaite proposer ce même service en confiant au client une partie de l'infogérance du service.

■ L'hébergeur est agréé pour l'hébergement d'une application nominativement désignée, mais souhaite héberger dans les mêmes conditions techniques toute application fournie par les clients et gérant des données de santé à caractère personnel.

LES SECONDES S'IMPOSENT À L'HÉBERGEUR, AFIN DE PRENDRE EN COMPTE L'ÉVOLUTION DU CADRE JURIDIQUE, DE L'ÉTAT DE L'ART TECHNIQUE ET DES DOCTRINES DE LA CNIL ET DU CAH

Pendant toute la durée d'agrément et, de surcroît, s'il en sollicite le renouvellement, l'hébergeur doit assurer une veille juridique et technique afin de maintenir un niveau de service à l'état de l'art et respectueux de la législation en vigueur. En outre, l'hébergeur doit également prendre en compte les doctrines de la CNIL et du CAH qui définissent les bonnes pratiques à respecter dans le cadre de l'hébergement de données de santé à caractère personnel.

Exemples d'évolutions que les hébergeurs doivent prendre en compte

■ Les dispositions de l'article L.1110-4 du code de la santé publique modifiées par la loi « HPST » du 21 juillet 2009 relatives à l'obligation pour les professionnels de santé d'utiliser une carte de professionnels de santé ou tout autre dispositif équivalent pour l'accès aux données de santé sur support informatique.

■ S'agissant de l'obligation d'assurer une veille technologique afin de garantir le respect de l'état de l'art, les deux points suivants doivent être pris en compte:
— évolution de la robustesse des mots de passe administrateurs: minimum 10 caractères comportant au moins une majuscule, une minuscule, un chiffre et un caractère spécial;
— nécessité de chiffrer les supports de sauvegardes externalisés.

■ **Le renforcement du contrôle du CAH sur les points suivants, dû à la présentation de prestations « génériques »:**
— nécessité de délimiter clairement le périmètre de la prestation d'hébergement et ne pas proposer une prestation de type « catalogue de services »;
— tout report d'obligation du décret, sur le client, doit être couvert contractuellement et être accompagné d'un réel devoir de conseil;
— nécessité de désigner les sous-traitants et de joindre les contrats de sous-traitance.

C - LE RAPPORT D'AUDIT EXTERNE DE SÉCURITÉ

L'article R.1111-15 du code de la santé publique précise que l'hébergeur doit joindre dans son dossier de demande de renouvellement d'agrément un rapport d'audit externe de sécurité attestant de la mise en œuvre de la politique de sécurité et de confidentialité définie à l'article R.1111-14 du même code.
Toutefois, cet article ne précise pas les modalités de réalisation de cet audit, ni les caractéristiques de l'auditeur.

Cette absence de précisions a entraîné de nombreuses interrogations et a ainsi conduit le CAH et l'ASIP Santé à publier un document d'aide à la réalisation des audits externes de sécurité visés à l'article R.1111-15 du code de la santé publique.

Le prestataire d'audit est au libre choix de l'hébergeur, qui pourra utilement se référer au référentiel de qualification publié par l'ANSSI, notamment dans ses volets audit d'architecture, audit de configuration et audit organisationnel et physique. L'hébergeur doit tout de même s'assurer du sérieux de l'auditeur auquel il recourt et de ses compétences en matière de sécurité des systèmes d'information.

S'agissant du contenu de l'audit, celui-ci doit couvrir les exigences du décret du 4 janvier 2006 et analyser le degré de conformité des moyens mis en œuvre par l'hébergeur au regard de ces exigences. Il ne suffit donc pas de se limiter à analyser la conformité des moyens mis en œuvre par l'hébergeur au regard de ce qu'il a déclaré dans son dossier de demande d'agrément initial. En outre, la conformité doit aussi être évaluée au regard des évolutions de l'état de l'art ayant pu émerger depuis la demande d'agrément initiale.

Observations sur certains audits reçus

■ Dans certains cas, l'auditeur ne réalise pas l'audit sur le périmètre complet du service agréé. Certaines thématiques du référentiel d'agrément (issues de l'article R.1111-14 du code de la santé publique) ne sont pas prises en compte.
— Un hébergeur a mis en place une nouvelle salle d'hébergement et cela n'a pas été pris en compte dans l'audit. De fait, il est difficile de savoir si les mesures de sécurité mises en œuvre sur cette nouvelle salle sont à l'état de l'art.
— Un auditeur a relevé des manquements sur la documentation avec, par exemple, un PAQ absent alors que le dossier de renouvellement présente un PAQ daté à une date antérieure à l'audit.
— Des auditeurs ont réalisé un audit de conformité à l'ISO 27799 et non au référentiel d'agrément.

■ Certains audits vérifient la conformité des moyens mis en œuvre par rapport à ce que le candidat a décrit dans son dossier de demande d'agrément initial, sans vérifier si ces moyens mis en œuvre permettent de répondre pleinement aux exigences du décret du 4 janvier 2006.

■ Certains audits ne sont pas accompagnés d'un plan de remédiation, alors que des non-conformités critiques sont parfois relevées dans ces audits.

■ L'audit externe devant être réalisé au regard des exigences du décret, il peut être étonnant de constater que certains auditeurs délivrent des rapports d'audit ne détectant aucune non-conformité, alors même que l'analyse du dossier et par la CNIL et le CAH relève des points d'attention.
— Par exemple, un auditeur a fourni un rapport ne relevant aucune non-conformité sur l'ensemble des exigences du décret et a conclu son rapport par « *À ce jour, aucune non-conformité n'existe vis-à-vis des exigences de l'ASIP pour l'agrément HDS* », ce qui peut sembler étonnant lorsque l'analyse du dossier initial aboutissait à un score de conformité de 69 % sur les 12 thématiques du décret.

L'audit doit également prendre en compte les recommandations qui accompagnaient la décision d'agrément et indiquer ce qui a ou non été mis en place par l'hébergeur pour les respecter. Le rapport d'audit externe doit être accompagné d'un plan d'actions décrivant ce que l'hébergeur s'engage à mettre en place et sous quels délais pour remédier aux points faibles relevés par l'auditeur.
Ces audits externes sont instruits par des experts en sécurité des systèmes d'information, qui comparent les résultats de l'analyse du dossier, avec les résultats de l'audit de sécurité. Les éventuels audits de complaisance peuvent donc être aisément détectés.

Les prestations d'hébergement de données de santé à caractère personnel sont à la croisée de différentes normes à respecter, techniques, juridiques, éthiques ou encore déontologiques, et les éléments que doit fournir l'hébergeur à l'appui de sa demande de renouvellement d'agrément démontrent la nécessité pour l'hébergeur de faire évoluer son offre de service dans le respect de ces normes.

La procédure d'agrément : une procédure nécessairement évolutive

Le cadre réglementaire tend à évoluer moins vite que les technologies. Dès lors, dans la perspective d'une éventuelle révision de la procédure pour l'améliorer et tenir compte des évolutions précédentes, le Comité s'intéressera à une formulation plus axée sur les objectifs poursuivis, avec une définition des moyens permettant à la fois l'encadrement visé et une acception suffisamment pérenne.

L'ESSENTIEL

Les hébergeurs doivent prendre en compte l'évolution des technologies pendant toute la durée de leur agrément afin de proposer un service à l'état de l'art (pour plus de précisions, cf. point A).

En parallèle, l'hébergeur doit également assurer une veille juridique afin de respecter les dispositions qui s'imposent à lui, mais également pour assurer son devoir de conseil auprès de ses clients (pour plus de précisions, cf. point B). Le patient devient un vrai acteur de sa santé et cela se constate par la multiplication des applications santé directement accessibles par le patient et qui doivent donc encadrer techniquement ces accès (pour plus de précisions, cf. point C).

A – L'ADAPTATION AUX ÉVOLUTIONS TECHNOLOGIQUES

La question des évolutions technologiques a un impact sur les modalités de réalisation de la fonction d'hébergement, mais aussi sur la protection des accès et la réalisation des modalités techniques de ces accès.

Les principaux points concernant l'hébergement sont relatifs, d'une part, aux techniques de chiffrement et, d'autre part, à la localisation des données de santé hébergées.

L'hébergeur doit donc prendre en compte la gestion des évolutions technologiques dans son dossier de demande d'agrément et assurer un devoir de conseil auprès de son client s'agissant de l'évolution des formats de données.

Concernant la localisation des données, l'évolution technologique, au travers de ce qu'on appelle communément le *cloud computing*, conduit à une banalisation des machines supports. L'avantage de cette technique est de pouvoir ajuster en permanence les capacités de ces machines aux besoins. L'inconvénient, c'est qu'il n'est plus possible, en tout cas pour certains types de solutions, de savoir où se trouvent les données à un instant « T ». Or, le décret du 4 janvier 2006 est rédigé de telle sorte que cette localisation est supposée maîtrisée. On perçoit donc que dans l'avenir, la question de l'accès, ou de l'accessibilité des données de santé, pourrait progressivement concentrer toute la vigilance des pouvoirs publics, tandis que la fonction d'hébergement proprement dite tend à échapper à tout contrôle du fait de l'impossibilité de localisation des données à protéger.

B – L'ADAPTATION AUX ÉVOLUTIONS LÉGISLATIVES

Conscient des difficultés techniques relatives à la mise en œuvre de la carte de professionnel de santé, notamment en situation de mobilité, le législateur a modifié **l'article L.1110-4** du code de la santé publique en introduisant la possibilité d'accéder aux données de santé à caractère personnel par carte de professionnel de santé (CPS) ou tout autre dispositif équivalent.

La carte CPS ne se présente donc plus comme la seule solution et d'autres solutions ont été reconnues. En effet, la dématérialisation accrue des données de santé, qui accompagne les nouveaux modes d'exercice de la médecine, conduit à rechercher d'autres moyens d'accès aux données de santé qui puissent s'adapter à ces situations et permettent de conserver le même niveau de sécurité que celui apporté par l'usage de la CPS, là où l'usage de celle-ci s'avère impossible ou mal adapté.

Il s'agit de couvrir les besoins d'authentification dans un plus grand nombre de contextes opérationnels.

Le terme « équivalent » n'est pas à prendre au sens littéral du terme, mais plutôt au regard du niveau de couverture des risques identifiés sur la globalité des composantes organisationnelles et techniques de la chaîne d'authentification.

Ainsi, ces solutions d'authentification équivalentes se fondent sur des dispositifs techniques alternatifs à la CPS, dont les caractéristiques techniques et les conditions d'utilisation conduisent à une couverture des risques identifiés équivalente à celle obtenue avec une carte CPS.

Les travaux que l'ASIP Santé a menés sur ce sujet, en particulier à l'occasion du DMP ou de la messagerie sécurisée de santé, ont permis d'identifier de tels dispositifs. De même, l'examen des dossiers déposés dans le cadre de la procédure d'agrément des hébergeurs a révélé des systèmes faisant appel à des dispositifs alternatifs à la CPS.

Article L.110-4

Modification de l'article introduite par la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires.

La procédure d'agrément : une procédure nécessairement évolutive

La liste des dispositifs alternatifs et de leurs conditions d'utilisation et de mise en œuvre est publiée par l'ASIP Santé dans le référentiel d'authentification des acteurs de santé de la PGSSI-S après validation par les autorités concernées. Elle est régulièrement mise à jour pour tenir compte des évolutions technologiques et de l'évolution des risques.

Quelques exemples de dispositifs alternatifs d'ores et déjà identifiés dans le référentiel d'authentification des acteurs de santé de la PGSSI-S et reconnus par le CAH dans le cadre de la procédure d'agrément.

■ L'UTILISATION D'UN CERTIFICAT LOGICIEL DE PERSONNE PHYSIQUE

Un certificat logiciel de personne physique issu de l'IGC Santé, c'est-à-dire adossé au RPPS, peut être retenu comme solution pragmatique et satisfaisante pour l'identification et l'authentification, dès lors que la commande de ce type de certificat s'appuie sur une authentification par carte CPS et que son confinement respecte les règles de l'art (notamment le déverrouillage spécifique par mot de passe). Ce mode d'authentification peut être retenu, puisqu'il constitue un mode d'authentification renforcé reposant à la fois sur un élément connu (code PIN du certificat) et un élément dont l'accès est détenu par la personne qui le met en œuvre (accès au support de confinement – généralement le magasin du système d'exploitation ou du navigateur Internet utilisé, ou un système de confinement spécifique).

■ L'UTILISATION D'UN COUPLE IDENTIFIANT/MOT DE PASSE ASSOCIÉ À UN CODE D'ACCÈS UNIQUE

L'authentification par mot de passe à usage unique (ou OTP: *One Time Password*) qui consiste à transmettre par courriel, SMS ou message vocal un mot de passe à l'utilisateur au moment où il effectue sa demande d'accès au service en ligne, constitue aujourd'hui un troisième dispositif sécurisé d'accès aux données de santé qui peut être retenu, dans la mesure où il constitue un mode d'authentification forte reposant à la fois sur un élément connu et un élément dont l'accès est détenu par la personne qui le met en œuvre.

Ce dispositif est d'ores et déjà opérationnel pour l'accès direct au dossier médical personnel par ses titulaires (accès patient). Il est également mis en œuvre pour la messagerie sécurisée de santé en alternative à la CPS dès lors qu'une première authentification avec la carte a été réalisée pour générer cet OTP.
Le mot de passe généré automatiquement par le service en ligne doit être saisi par l'utilisateur et n'est valable que pour une seule session.

Une variante spécifique aux applications sur téléphones et tablettes connectés consiste à transmettre l'OTP directement à l'application cliente via le canal de signalisation de la téléphonie mobile, sans ressaisie de l'OTP par l'utilisateur. Cette variante est appelée OTP *push* et présente, du point de vue de la sécurité les mêmes caractéristiques que la transmission de l'OTP et sa ressaisie par l'utilisateur. Le mécanisme d'authentification par mot de passe à usage unique requiert une phase « d'enrôlement » préalable de tout utilisateur.

Notons que la CNIL, dans sa délibération du 25 avril 2013 sur le service national de messagerie sécurisée de santé, a considéré que les mesures ainsi mises en place « *[…] qui apparaissent conformes aux dispositions de l'article L.1110-4 du code de la santé publique, sont de nature à garantir une authentification fiable des émetteurs et destinataires des messages.* » Ce système apparaît utile aujourd'hui pour le développement des nouveaux modes d'exercice des professionnels de santé notamment en situation de mobilité.

Ces trois modes d'authentification susceptibles d'être reconnus comme des dispositifs alternatifs à la CPS ne sont clairement pas du même niveau de sécurité que l'authentification par CPS. Toutefois, les risques résiduels supplémentaires induits par l'utilisation d'un de ces modes apparaissent mesurés et acceptables. Leur reconnaissance permet de réduire considérablement les usages où, faute de CPS, aucune sécurité acceptable n'est mise en œuvre.

Le Comité d'agrément et la CNIL ont d'ores et déjà émis des avis favorables pour des services d'hébergement de données de santé qui présentaient, à défaut de CPS, l'utilisation d'un identifiant/mot de passe associé à un mot de passe à usage unique ou encore l'utilisation d'un certificat serveur applicatif délivré à une structure de soins, associé à un identifiant/mot de passe utilisé par la personne physique et délivré par le directeur de la structure de soins au sein de laquelle celle-ci exerce.
Les moyens d'authentification alternatifs à la CPS doivent être conformes à la politique générale de sécurité des systèmes d'information de santé **[PGSSI-S]**.

PGSSI-S
Pour en savoir plus :
esante.gouv.fr/pgssi-s/presentation

C – L'ADAPTATION DE LA PROCÉDURE D'AGRÉMENT AUX NOUVELLES OFFRES DE SERVICES ACCESSIBLES DIRECTEMENT PAR LE PATIENT

L'évolution générale de la société est celle d'un citoyen-patient à la fois responsable de sa santé et équipé d'un ou plusieurs équipements numériques portables.
Le développement de la e-santé a conduit ainsi à l'émergence de services collectant des données de santé à caractère personnel, directement accessibles aux patients.
Les questions d'authentification prennent dans ce contexte une importance particulière et l'accès du patient aux données de santé – comme de tout autre acteur habilité – doit donc être réalisé de façon sécurisée.

À titre d'exemple, dans le cadre de la télésurveillance médicale (acte de télémédecine au sens du décret 2010-1229 du 19 octobre 2010), la transmission des données de santé au professionnel de santé prenant en charge le patient peut être réalisée par le patient lui-même. À cet effet, de nombreux dispositifs médicaux sont aujourd'hui associés à des services à valeur ajoutée qui permettent au professionnel de santé d'avoir accès de façon simple et rapide aux données produites ou collectées à l'appui du dispositif médical. Prenons l'exemple d'un patient diabétique qui utilise un glucomètre : le glucomètre est connecté à une application sur Internet vers laquelle vont automatiquement être transférés les différents taux de glucose calculés par le glucomètre. Le patient doit ensuite se connecter à l'application afin de renseigner des informations nutritionnelles (indiquer ce qu'il a mangé) et toute autre information utile à porter à la connaissance du professionnel de santé. Le professionnel de santé pourra ainsi suivre la glycémie du patient à distance et en temps réel en se connectant à l'application.

L'application collecte des données de santé à caractère personnel produites à l'occasion d'une activité de soins et doit ainsi respecter l'ensemble des dispositions législatives, dont la nécessité de garantir la sécurité et la confidentialité des données de santé. L'un des moyens de garantir la confidentialité des données de santé concerne les moyens d'accès et donc d'authentification aux données de santé. Les professionnels de santé qui accèdent à l'application de télésurveillance médicale doivent utiliser une carte CPS ou tout autre dispositif équivalent. S'agissant des patients, des moyens d'authentification de même niveau doivent être mis en œuvre afin de préserver la sécurité des données de santé. Pour l'accès à l'application de télésurveillance, le patient devra donc se voir délivrer des moyens d'authentification forte *(cf. page 17)*.

Un autre exemple qui a fait l'actualité de ces derniers mois a trait aux sites de vente en ligne de médicaments. L'arrêté du 20 juin 2013 relatif aux bonnes pratiques de dispensation de médicaments par voie électronique impose au pharmacien qui souhaite dispenser des médicaments par Internet de prévoir sur son site (la création des sites de vente en ligne de médicaments nécessite une autorisation de l'Agence régionale de santé) un espace « Mon compte » sur lequel le patient devra s'identifier et s'authentifier pour commander des médicaments. Le patient doit renseigner sur ce site des informations relatives à son état de santé afin que le pharmacien puisse assurer son devoir de conseil dans le cadre de la dispensation de médicaments. Ces sites doivent donc prévoir un « accès patient » et remettre à cet effet au patient un moyen d'authentification forte pour s'y connecter.
L'arrêté du 20 juin 2013 précité indique que des données de santé à caractère personnel sont collectées par les sites en vente en ligne

de médicaments et que, dès lors, leur hébergement (cas où le pharmacien confie à un tiers l'hébergement du site) doit être réalisé par un prestataire agréé pour l'hébergement de **données de santé**.

Au regard des caractéristiques de l'hébergement des données de santé collectées par les sites de vente en ligne de médicaments, deux types d'agrément, aujourd'hui délivrés, répondent aux exigences requises par les textes précités.

— L'agrément pour une prestation visant explicitement l'hébergement de sites de vente en ligne de médicaments avec possibilité d'accès du direct patient à l'application au moyen d'un dispositif d'authentification forte.

— L'agrément pour l'hébergement d'applications de gestion de données de santé à caractère personnel, utilisées à des fins de suivi médical, avec possibilité pour le patient d'accéder directement à l'application au moyen d'un dispositif d'authentification forte (agrément dit « générique »).

Si l'hébergeur souhaite proposer une prestation d'hébergement de données de santé à caractère personnel collectées au moyen d'applications directement accessibles par le patient (cas notamment des sites de vente en ligne de médicaments), son dossier de demande d'agrément doit prendre en compte cette fonctionnalité d'accès direct.

Données de santé

Cf. Instruction n° DGS/DSSIS/2014/172 du 28 mai 2014 relative à l'hébergement de données de santé à caractère personnel dans le cadre de la dispensation par Internet de médicaments à usage humain.

Ce que doit renseigner l'hébergeur dans son dossier de demande d'agrément

L'hébergeur doit indiquer dans son dossier de demande d'agrément les moyens mis en œuvre pour contrôler les accès aux données de santé qu'il héberge. On peut distinguer trois grandes catégories d'accès.

1 - Les personnels techniques

Ces accès doivent être encadrés par une gestion fine des habilitations. Les personnels doivent être sensibilisés à la gestion des données de santé et avoir a minima une clause de confidentialité dans leur contrat de travail.

Ils doivent utiliser des comptes d'accès individuels et être dotés des moyens d'authentification conformes à l'état de l'art :
— identifiant/mot de passe conforme aux recommandations de la CNIL (10 caractères minimum avec au moins une majuscule, une minuscule, un chiffre ou un caractère spécial) ;
— moyens d'authentification forte (cartes à puce, comme, par exemple, des cartes de personnel autorisé (CPA), biométrie, etc.).

Les accès des personnels techniques doivent être tracés.

2 - Les professionnels de santé

Le contrat d'hébergement doit indiquer qui, de l'hébergeur ou de son client, est responsable de la gestion des habilitations des professionnels de santé.
En tout état de cause, le modèle de contrat doit imposer l'utilisation par les professionnels de santé de moyens d'authentification forte par carte CPS ou tout autre dispositif équivalent. La responsabilité du contrôle de l'utilisation de ces moyens relèvera soit de l'hébergeur, soit de son client (selon la répartition des responsabilités définie dans le contrat).

3 - Les patients

Lorsque les applications hébergées sont directement accessibles par le patient, le dossier de demande d'agrément doit clairement présenter cette fonctionnalité.

■ Identification

Le dossier de demande d'agrément doit préciser les moyens mis en œuvre pour réaliser l'enrôlement du patient.
Les procédés suivis doivent notamment assurer l'attribution du bon identifiant au bon patient afin d'éviter les doublons et les risques de collision entre des dossiers de différents patients.

Lorsque l'hébergeur n'est pas en lien direct avec le patient, il doit clairement définir les principes que s'engage à respecter son client afin de garantir l'identification du patient.

■ Authentification

Il est impératif d'utiliser un moyen d'authentification forte afin de préserver la sécurité des accès.
Plusieurs moyens d'authentification forte peuvent être mis en œuvre par l'hébergeur ou son client.

À titre d'exemple, voici quelques moyens qui peuvent être retenus :
— utilisation d'un identifiant/passe associé à un mot de passe à usage unique (OTP = *One Time Password*) envoyé par e-mail ou SMS ;
— utilisation d'un certificat électronique de type carte à puce.

03

La protection des données de santé du citoyen : pierre angulaire de l'instruction des dossiers de demande d'agrément

L'ESSENTIEL

L'utilisation croissante des NTIC dans le domaine de la santé nécessite de mettre en œuvre les mesures adéquates pour préserver les droits des patients (pour plus de précisions cf. point A).

Le CAH s'est toutefois aperçu que l'obligation de recueillir le consentement du patient pour l'hébergement de ses données de santé était en pratique difficile à respecter.
Le CAH propose donc une évolution des textes sur ce point (pour plus de précisions cf. point B).
Pour concourir au respect des droits des patients dont les données sont hébergées, l'hébergeur est tenu de désigner un médecin. Les missions de ce médecin ne sont pas définies par les textes. Le Conseil national de l'ordre des médecins a publié sur son site Internet un modèle de contrat « médecin de l'hébergeur » qui définit les missions de ce dernier *(pour plus de précisions cf. point C).*

Actualité
Le futur projet de loi de santé publique qui devrait être présenté au Parlement début 2015 propose des modifications de l'article L.1111-8 du code de la santé publique dont les deux dispositions suivantes.
■ La suppression de l'exigence du recueil du consentement exprès de la personne concernée par l'hébergement de ses données de santé.
■ La définition d'un fondement législatif à la possibilité pour le médecin de l'hébergeur d'accéder aux données de santé à caractère personnel dans le cadre de ses missions.
La réflexion se poursuit également sur les modalités selon lesquelles la procédure d'agrément pourrait être améliorée au regard des évolutions intervenues depuis cinq ans.

A – LES ÉVOLUTIONS TECHNIQUES ET L'USAGE CROISSANT DE L'INFORMATIQUE DANS LE DOMAINE DE LA SANTÉ IMPOSENT LA MISE EN PLACE DE NOUVEAUX SCHÉMAS ORGANISATIONNELS AFIN DE PROTÉGER LES CITOYENS

Lorsque le décret du 4 janvier 2006 a été pris en application des dispositions de la loi, les pouvoirs publics ont souhaité que des représentants de patients soient associés au processus d'agrément, marquant ainsi leur volonté de placer cette nouvelle procédure au cœur de la protection des données de santé des citoyens. C'est ainsi que les patients sont représentés au CAH par deux membres titulaires provenant d'associations de patients.

Rappelons que les données personnelles de santé qui permettent d'identifier un individu sont des données sensibles susceptibles de révéler l'intimité de la vie privée. À ce titre, le droit leur reconnaît un statut particulier et impose le respect de règles ayant pour objectif de garantir leur confidentialité.

L'information préalable de la personne sur l'informatisation de ses données et, en particulier, l'information sur ses droits représentent toujours une garantie importante. La loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés en a posé le principe et la CNIL en contrôle l'effectivité.

Dans certains cas, le recueil du consentement peut être une protection supplémentaire de la personne. Le code de la santé publique et le code de la sécurité sociale comportent des dispositions qui exigent le recueil de ce consentement exprimé ou pas de façon expresse ou matérialisé et souvent demandé de façon différente selon les projets, ce qui ne facilite pas la lecture et la compréhension du citoyen et des acteurs du secteur.

Le code pénal incrimine toujours la révélation d'une **information à caractère secret** par une personne qui en est dépositaire soit par état, soit par profession, soit en raison d'une fonction ou d'une mission temporaire.

Le développement des systèmes d'information partagés de données de santé, intervenu maintenant depuis une dizaine d'années, multiplie les architectures possibles (développement du *cloud computing*, recours accru aux dispositifs mobiles…) et accroît encore davantage la nécessité de garantir à la personne que ses propres données ne seront pas communiquées à des tiers non autorisés.

La technique doit alors prendre le relais du droit. Comment garantir aujourd'hui la confidentialité des données de santé personnelles, en continuant à délivrer aux patients une information claire et surtout intelligible ?

La garantie d'un encadrement juridique important des données personnelles de santé doit aujourd'hui se décliner en pratique à travers la définition des conditions d'une protection efficace, sûre et adaptée aux cas d'usage de la médecine, permettant au citoyen d'être confiant dans la gestion d'un système de santé de qualité.

⊠

Information à caractère secret

Cf. article 226-13 du code pénal.

Les travaux conduits par le Comité d'agrément des hébergeurs sont à cet égard essentiels.

Lorsque le professionnel ou l'établissement de santé recourt à un hébergeur agréé, il est tenu d'informer le patient sur les conditions dans lesquelles il peut exercer ses droits d'accès, de rectification et d'opposition, de recueillir son consentement exprès à l'hébergement de ses données de santé et enfin de l'informer en cas d'accès frauduleux à ses données.

Entre autres, ces informations doivent être données aux patients de façon systématique soit par voie d'affichage dans tous les lieux de soins, soit par la remise d'une brochure lors de la première consultation. Cette démarche nécessite d'être complétée par une information orale afin de s'assurer que le patient a bien compris les éléments qui lui sont fournis. La mise en œuvre de ces obligations, aussi délicate soit-elle, doit être respectée par les professionnels et établissements de santé afin de garantir au patient l'exercice effectif de ses droits.

Afin que ce dispositif soit incontestable, tous les acteurs de santé doivent être conscients de leurs obligations. Seul le respect scrupuleux de la réglementation amènera l'adhésion des citoyens à une organisation des soins qui se veut soucieuse du respect de la personne humaine.

La prise en compte des droits des patients est donc essentielle pour le développement de la e-santé. Toutefois, au regard des différents types de services aujourd'hui proposés – qui ne se limitent plus à l'hébergement de dossiers patients informatisés – et des conditions d'hébergement des données de santé, le Comité d'agrément constate que, si l'information du patient s'agissant des conditions d'hébergement de ses données de santé est essentielle, l'obligation de recueillir son consentement exprès en cas de recours à un hébergeur agréé est dans de nombreux cas très délicate à respecter.

B – LE CONSENTEMENT À L'HÉBERGEMENT DE SES DONNÉES DE SANTÉ À CARACTÈRE PERSONNEL : UNE OBLIGATION DÉLICATE, VOIRE IMPOSSIBLE A RESPECTER EN PRATIQUE

La loi (article L.1111-8 alinéa 1er du code de la santé publique) indique que l'hébergement de données de santé à caractère personnel, quel qu'en soit le support, papier ou informatique, ne peut avoir lieu qu'avec le consentement exprès de la personne concernée.

Le contrôle du recueil du consentement exprès à l'hébergement de ses données de santé est réalisé par la CNIL. Le CAH vérifie également ce point dans le cadre de l'examen du contrat d'hébergement conclu entre l'hébergeur et son client. En effet, ce contrat doit comporter une clause précisant quelle partie au contrat est responsable du recueil de ce consentement. Dans la majorité des dossiers analysés par le CAH, cette obligation est logiquement à la charge du professionnel ou de l'établissement de santé, en lien direct avec le patient. Le report de cette obligation sur le professionnel ou l'établissement de santé doit être accompagné d'un devoir de conseil de l'hébergeur. Certains hébergeurs vont même jusqu'à exercer un contrôle de la mise en œuvre de cette obligation sur leurs clients.

Si la finalité des textes relatifs à l'hébergement de données de santé et la nécessité de prendre en compte le respect des droits des personnes rencontrent une adhésion croissante des professionnels de santé, les modalités de mise en œuvre de ces droits ne sont pas toujours simples.

L'information du patient n'est-elle pas considérée par les professionnels ou les établissements de santé comme accessoire au recueil du consentement ? Le patient est-il à même de comprendre les spécificités des différentes étapes pour lesquelles il lui est demandé de donner son consentement ? On rappellera notamment l'ambiguïté de la remise de la carte Vitale pour la consultation de l'historique des remboursements.

Enfin, est-il nécessaire de solenniser l'accord du patient pour l'hébergement de ses données de santé, alors que le législateur a mis en place au moyen de la procédure d'agrément des garanties très fortes de sécurité et de confidentialité ?

Ne faudrait-il pas privilégier l'information du patient sur le fonctionnement du système de santé et les garanties qui y sont attachées et revaloriser ainsi l'information qui lui est due et le droit d'opposition, plutôt que de superposer des régimes de consentement ? Question désormais récurrente.

Il convient de noter que les dérogations au recueil du consentement exprès à l'hébergement des données de santé à caractère personnel se sont multipliées et sont de nature à remettre en cause la nécessité d'une telle obligation.

Ainsi, l'article L.1111-8 alinéa 5 dispose que le recueil du consentement n'est pas nécessaire dès lors que les données de santé hébergées sont accessibles au seul professionnel de santé qui les dépose auprès d'un hébergeur agréé.

En outre, l'article 29 de la loi ° 2011-940 du 10 août 2011 modifiant certaines dispositions de la loi n° 2009-879 du 21 juillet 2009 portant réforme de l'hôpital et relative aux patients, à la santé et aux territoires a posé une nouvelle dérogation qui consiste à considérer que *« pour l'application de l'article L.1111-8 du code de la santé publique, le consentement exprès des personnes concernées est, à compter de la promulgation de la présente loi, réputé accordé pour ce qui concerne le transfert des données de santé à caractère personnel actuellement hébergées par les établissements publics de santé et par les établissements de santé privés ».*

Cette question est d'autant plus prégnante qu'il apparaît illusoire de pouvoir respecter en pratique le droit d'opposition du patient à l'égard de l'hébergement externalisé de ses données. En effet, au-delà de la question de la réalité d'un véritable choix offert au patient, si celui-ci s'oppose à l'hébergement de ses données de santé auprès d'un hébergeur agréé, cela implique pour le responsable de traitement de conserver les données de santé du patient localement, sous format papier ou électronique et donc souvent dans des conditions de sécurité moins efficientes.

La volonté de faire appel à un hébergeur agréé est en effet souvent justifiée par les difficultés auxquelles se trouvent confrontés les professionnels et établissements de santé de conserver de façon sécurisée les données de santé des patients qu'ils prennent en charge.

Le déploiement actuel de la messagerie sécurisée de santé (MSSanté) permet d'illustrer ce point.

En effet, le respect du recueil du consentement exprès est difficilement possible lorsque les données sont échangées par voie de messagerie électronique sécurisée. Cette obligation qui pèse sur l'hébergeur incomberait en pratique à chaque professionnel de santé qui devrait solliciter le consentement du patient à l'hébergement de ses données avant l'envoi de chaque message électronique. Les conditions d'usage de la messagerie, le plus souvent hors la présence du patient, rendent impossible le respect de cette exigence.

À cet égard, dans sa délibération du 25 avril 2013 autorisant la mise en œuvre par l'ASIP Santé du système de messageries MSSanté, la CNIL a reconnu qu'il n'était pas réaliste d'exiger un recueil du consentement à chaque échange ou pour chaque destinataire et a donc admis une dérogation au recueil du consentement pour ces raisons. La CNIL a également souligné que les réflexions sur les évolutions du cadre juridique propre à l'hébergement au sein du Comité d'agrément des hébergeurs et dans le cadre de la PGSSI-S conduisaient à proposer une modification de l'article L.1111-8 sur ce point. La loi pourrait ainsi venir remplacer l'exigence du recueil du consentement exprès par un régime plus adapté à la réalité des pratiques. Le patient serait alors informé que les données de santé le concernant sont hébergées auprès d'un hébergeur agréé et qu'il peut exercer ses droits d'accès et de rectification.

Ce que doit renseigner l'hébergeur dans son dossier de demande d'agrément

■ Le candidat à l'agrément doit prendre en compte dans son dossier de demande d'agrément la nature particulièrement sensible des données de santé à caractère personnel et ainsi adapter son service aux obligations définies par les articles L.1111-8 et R.1111-9 et suivants du code de la santé publique.

■ Le dossier de demande d'agrément doit clairement présenter les moyens mis en œuvre pour garantir l'effectivité des droits des personnes.

■ Le contrat d'hébergement doit clairement indiquer qui, de l'hébergeur ou de son client, est responsable de la mise en œuvre du respect des droits des patients (information, recueil du consentement, prise en compte des demandes d'accès aux données de santé, etc.).

■ Lorsque le respect des droits des patients est reporté sur le client de l'hébergeur, ce report doit être accompagné d'un devoir de conseil de l'hébergeur.

À titre d'exemple, l'hébergeur peut annexer au modèle de contrat d'hébergement un modèle de note d'information.

C - LE MÉDECIN DE L'HÉBERGEUR : GARANT DE LA CONFIDENTIALITÉ DES DONNÉES DE SANTÉ

Une des exigences du décret 2006-6 du 4 janvier 2006 impose à l'hébergeur d'identifier parmi les personnes en charge de l'activité d'hébergement, un médecin (article R.1111-9 du code de la santé publique). Un contrat passé entre l'hébergeur et le médecin désigné précise ses fonctions.

La CAH a progressivement dégagé une doctrine sur le rôle du médecin de l'hébergeur. Les clauses contractuelles types devant figurer dans les contrats conclus entre l'hébergeur et le médecin ont été publiées sur le site de l'ASIP Santé et du Conseil national de l'ordre des médecins.

Ce médecin veille à la confidentialité des données de santé à caractère personnel hébergées et au respect des conditions d'accès aux données dans le respect de la loi Informatique et Libertés et du code de la santé publique. Garant du secret professionnel, il peut accéder aux données de santé à caractère personnel hébergées dès lors que l'accomplissement de ses missions l'impose.

Le médecin de l'hébergeur doit également veiller à ce que le personnel de l'hébergeur (ou de ses sous-traitants) ne puisse pas accéder aux données de santé hébergées, sauf lorsque de tels accès sont nécessaires pour l'exercice de leurs missions.

Si dans le strict cadre de leurs missions de maintenance ou d'administration, les administrateurs peuvent avoir accès à des données de santé en clair, ces accès doivent être réalisés sous le contrôle du médecin de l'hébergeur (gestion des listes d'administrateurs habilités, sensibilisation à la confidentialité des données de santé, etc.).

Le médecin de l'hébergeur doit également être impliqué en cas d'incident sur les données de santé. Il doit par exemple être membre des comités de gestion/résolution d'incidents.
Le rôle du médecin de l'hébergeur varie en fonction du service d'hébergement proposé par l'hébergeur.

Ce que doit renseigner l'hébergeur dans son dossier de demande d'agrément

- Le candidat doit renseigner le nom du médecin de l'hébergeur et la nature du lien juridique (formulaire P1).
- Le candidat doit également joindre dans son dossier de demande d'agrément le contrat conclu avec le médecin de l'hébergeur.
- Il est fortement recommandé d'utiliser le modèle de contrat « médecin de l'hébergeur » publié par le Conseil national de l'ordre des médecins.
- Le médecin de l'hébergeur désigné par l'hébergeur doit avoir un lien avec l'hébergeur qui lui permette d'exercer ses missions en toute objectivité. Ainsi, les liens d'intérêt entre le médecin de l'hébergeur et les organes dirigeants du candidat ne doivent pas remettre en cause l'indépendance et l'objectivité du médecin pour l'exercice de ses fonctions.
- Par exemple, désigner le président-directeur général d'une société comme médecin de l'hébergeur ne permet pas de répondre à cette obligation d'indépendance.
- Lorsque des administrateurs peuvent avoir accès aux données de santé à caractère personnel hébergées en clair dans le strict cadre de leurs missions (administration, maintenance, etc.), ces accès doivent être réalisés sous le contrôle du médecin de l'hébergeur. Ce point doit être décrit dans les dossiers de demande d'agrément.

Le Comité d'agrément relève qu'aujourd'hui aucun texte ne définit le rôle du médecin de l'hébergeur et qu'il est nécessaire que le législateur intervienne afin de consacrer explicitement la possibilité d'accès pour le médecin de l'hébergeur aux données hébergées dans le cadre de ses missions.

Le respect des droits des personnes est un axe important des dossiers de demande d'agrément apprécié au regard de la finalité de la prestation d'hébergement de données de santé à caractère personnel. La définition du service, objet du dossier de demande d'agrément et, en amont du périmètre des prestations concernées par la procédure d'agrément sont des interrogations récurrentes que le CAH, la CNIL et l'ASIP Santé essaient de résoudre au fil de l'instruction et de l'examen des dossiers reçus.

04

Le périmètre de la procédure d'agrément : une appréciation guidée par la protection des données de santé

L'ESSENTIEL

L'article L.1111-8 du code de la santé publique a pour finalité la protection des données de santé dès lors qu'elles sont « hébergées » chez un tiers.

Le contrat d'hébergement doit permettre d'encadrer les relations entre les parties et de garantir le respect des droits des personnes concernées par les données de santé (pour plus de précisions, cf. point A).

La CNIL et le CAH ont une interprétation large de l'article L.1111-8 du code de la santé publique *(pour plus de précisions, cf. points B, C, D et E)*, mais sont conduits à devoir s'interroger régulièrement sur la recevabilité d'une demande.

La question s'est notamment posée pour les prestations de type « salle blanche » *(pour plus de précisions, cf. point C)*.

Le périmètre d'application de l'article L.1111-8 du code de la santé publique est une question récurrente.

Le Comité d'agrément est conduit de plus en plus souvent à devoir se prononcer sur la recevabilité d'un dossier de demande d'agrément au regard de la catégorie du demandeur, de la nature des données hébergées ou encore du service d'hébergement proposé, avant même d'analyser le contenu du dossier.

L'alinéa 1 de l'article L.1111-8 du code de la santé publique indique uniquement que *« les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet ».*

Le terme « d'hébergement », qui n'est pas défini de façon précise dans les textes, recouvre une réalité complexe. L'hébergement de données n'est pas nécessairement un but en soi et est le plus souvent associé à la mise en œuvre de logiciels applicatifs qui exploitent ou produisent ces données. La nécessité d'assurer la disponibilité et la pérennité de ces données et de protéger leur accès, génère des fonctions techniques supplémentaires comme la mise en place de sites de secours ou encore le chiffrement des données, réseaux sécurisés, etc.

Il apparaît que le patient, dont la protection des données de santé constitue l'enjeu principal du décret, est au bout de la chaîne de valeur et rarement lié directement à l'hébergeur. Les acteurs qui maîtrisent cette relation sont le plus souvent les gestionnaires d'application, qu'ils soient des professionnels de santé, des structures de soins ou des opérateurs intervenant pour le compte de professionnels indépendants ou engagés dans des activités de recherche ou périphériques aux soins. Les obligations que la réglementation impose à l'hébergeur autour des droits du patient ne peuvent donc être assurées directement par lui, mais seulement par le moyen de clauses contractuelles et de son devoir de conseil.

Le contrat d'hébergement de données de santé à caractère personnel est un élément essentiel du dossier de demande d'agrément (article R.1111-13 du code de la santé publique).

A - L'ENCADREMENT DES LIENS ENTRE LES ACTEURS PAR LE CONTRAT D'HÉBERGEMENT

Dans le cadre de l'analyse des dossiers de demande d'agrément, le Comité d'agrément constate régulièrement que le modèle de contrat d'hébergement est souvent moins bien traité au profit de la description des moyens techniques mis en œuvre. Or, ce contrat est la pièce maîtresse du dossier de demande d'agrément.

L'objet du contrat liant l'hébergeur à son client doit être rédigé de façon claire et précise, de façon à ce que l'étendue et la finalité de la prestation d'hébergement puissent être appréciées. Il en est de même des autres clauses qui doivent préciser la manière dont l'hébergeur exercera ses obligations et respectera les droits des personnes concernées.

La répartition des responsabilités entre l'hébergeur et son client doit être claire.
Le modèle de contrat doit tenir compte de la nature des données (données sensibles) et prévoir les modalités pour que soient garanties la sécurité et la confidentialité de ces données. Le contrat doit imposer de façon explicite l'utilisation de la CPS ou de tout procédé équivalent. Il est important de rappeler que le candidat doit décrire dans le modèle de contrat les moyens mis en œuvre pour la fourniture des services.
Le contrat ne doit pas laisser optionnels des prestations ou services inhérents aux obligations de l'hébergeur comme, par exemple, l'organisation de la disponibilité et de la continuité du service (délai de rétablissement du service) ou encore la sauvegarde des données de santé sur un site distant.

Le contrat doit toujours être fourni avec ses annexes quand celles-ci concourent à la description de la prestation et à la définition des éléments exposés ci-dessus.

En sa qualité d'hébergeur agréé pour l'hébergement de données de santé à caractère personnel, l'hébergeur doit exercer son devoir de conseil auprès de son client, adapté à la finalité de la prestation, à la sensibilité des données de santé et aux besoins du client.

Ce que doit renseigner l'hébergeur dans son dossier de demande d'agrément

Le modèle de contrat d'hébergement doit comporter les clauses prévues à l'article R.1111-13 du code de la santé publique.
Le contrat doit notamment :

- être adapté à une prestation d'hébergement de données de santé à caractère personnel et donc prendre en compte le respect des droits des personnes ;
- clairement définir le périmètre de la prestation d'hébergement objet du contrat et, donc, du dossier de demande d'agrément ;
- présenter avec précision la répartition des responsabilités entre l'hébergeur et son client (un document de type « matrice de responsabilités » peut compléter le contrat) ;
- indiquer les typologies de clients à qui la prestation est proposée ;
- indiquer les moyens que doivent utiliser les utilisateurs finaux pour accéder aux données de santé à caractère personnel : l'utilisation de la carte de professionnel de santé ou de tout autre dispositif équivalent doit être imposée.

Le contrat d'hébergement ne doit pas être présenté sous la forme d'une sorte de « catalogue de services », puisque le candidat à l'agrément est tenu de définir le périmètre du service d'hébergement pour lequel il souhaite être agréé et indiquer les moyens mis en œuvre pour proposer ce service.

Exemples de clauses souvent faibles dans les modèles de contrat

■ **La description des moyens** mis en œuvre pour la fourniture de la prestation est souvent lacunaire. Le contrat d'hébergement doit présenter les grandes lignes des moyens mis en œuvre.

■ **La mention des indicateurs de services** fait souvent défaut, alors même que cela permet d'apprécier la capacité de l'hébergeur à assurer la disponibilité et la continuité du service. Ces niveaux de services doivent être adaptés à la finalité de la prestation et aux besoins des clients (exemple : lorsque le client est un CHU, l'hébergeur doit pouvoir proposer une prise en compte des incidents en 24/7).

■ **À propos des clauses excluant la responsabilité du candidat pour des intrusions frauduleuses,** il convient de faire la distinction entre des intrusions frauduleuses de tiers pour lesquelles l'exclusion de responsabilité peut être valable et les possibles intrusions frauduleuses du personnel de l'hébergeur. L'obligation de sécurité est en tout état de cause une obligation de moyens.

■ **Il convient de décrire les mesures à mettre en œuvre** en cas de résiliation du contrat.

■ **Il est nécessaire d'identifier clairement** les personnes habilitées à accéder aux données.

■ **Dès lors que l'hébergeur ne fournit pas l'applicatif métier,** le contrat d'hébergement doit reporter la responsabilité de la traçabilité applicative sur le client en précisant les types d'actions que l'application doit tracer.

■ **L'ensemble des points suivants doit également être décrit :** information des patients, politique d'habilitation, fonctions des personnels qui interviennent pour la maintenance, modalités d'une cession du contrat (y compris l'obligation de céder celui-ci à un hébergeur agréé).

Le modèle de contrat d'hébergement permet de définir le périmètre de la prestation d'hébergement de données de santé, d'encadrer les relations entre les parties et de garantir le respect des droits des personnes concernées par les données de santé hébergées. C'est dans cet objectif de protection des données de santé et des droits des personnes que la CNIL et le CAH ont une interprétation large de la notion *« d'hébergement de données de santé à caractère personnel »*.

B – L'INTERPRÉTATION LARGE DE LA NOTION D'HÉBERGEMENT DE DONNÉES DE SANTÉ NÉCESSITANT UN AGRÉMENT

L'article L.1111-8 du code de la santé publique vise les professionnels de santé, les établissements et la personne concernée comme devant recourir à un hébergeur agréé à cet effet en cas d'externalisation de l'hébergement de données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic ou de soins.

Selon le Comité d'agrément, l'utilisation par le législateur de la seule notion de « professionnel de santé » permet d'éviter l'écueil des listes qui se veulent exhaustives sans réellement y parvenir et ainsi de s'adapter à toutes les situations d'exercice de ces professionnels – activité libérale individuelle ou de groupe, activité salariée au sein de toute structure de soins – afin d'appliquer les dispositions de l'article L.1111-8 du code de la santé publique précisées par le décret 2006-6 du 4 janvier 2006.

En effet, même si cet article distingue les notions d'établissements de santé et de professionnels de santé, il ne précise pas que la notion de « professionnel de santé » vise uniquement les professionnels de santé exerçant à titre libéral en cabinet individuel. Ce texte n'exclut pas non plus les structures de soins ou de prise en charge de patients et d'usagers, qui n'entrent pas dans la définition de l'établissement de santé au sens des articles L.6111-1 et suivants du code de la santé publique, et au sein desquelles des données de santé à caractère personnel sont recueillies par les professionnels qu'elles engagent.

À cet égard, le Comité d'agrément et la CNIL ont déjà eu à se prononcer sur des dossiers de demande d'agrément relatifs à l'hébergement de données de santé à caractère personnel collectées par des établissements d'hébergement pour personnes âgées dépendantes (EHPAD), des services de santé au travail, des fédérations sportives ou encore par un groupement d'organismes d'assurance maladie complémentaire.

Aujourd'hui, le parcours de soins d'un patient est souvent pluridisciplinaire et fait intervenir de nombreux acteurs qui ne sont pas des professionnels de santé, mais qui sont amenés à collecter des données de santé à caractère personnel dans le cadre de leurs missions. Citons ainsi le cas des prestataires de services de santé à domicile qui délivrent des dispositifs médicaux et doivent en assurer la surveillance. Bien que le prestataire de services de santé à domicile ne soit ni un professionnel de santé ni un établissement de santé au sens du code de la santé publique, il est tenu dans le cadre de ses missions de collecter des données de santé relatives aux personnes prises en charge. Dès lors que ce prestataire de services de santé à domicile souhaite externaliser la conservation des dossiers des personnes bénéficiaires des dispositifs médicaux qu'il délivre, le CAH et la CNIL ont considéré qu'il devait faire appel à un hébergeur agréé pour l'hébergement de données de santé.
La CNIL et le CAH estiment que la conservation des données de santé collectées par les établissements médico-sociaux, les centres de santé, les laboratoires de biologie médicale et, plus largement, toute structure réalisant des missions de prévention, de diagnostic ou de soins dès lors qu'elle est externalisée, doit être confiée à un hébergeur agréé.

La protection des données de santé à caractère personnel de l'ensemble des citoyens, quelle que soit la nature juridique de l'organisme qui les collecte, est le fondement de cette interprétation. À l'heure où certains s'émeuvent de façon légitime de l'absence de garanties pour la personne de la conservation sur Internet de leurs données par des organismes qui proposent des services attrayants, la procédure d'agrément prévue par la loi française apparaît comme une protection importante. Elle est d'ailleurs reconnue par les autres pays,

notamment européens, qui se sont dotés ou se dotent également aujourd'hui des moyens de protéger les données de santé de leurs citoyens.
Il ne doit pas être répondu à la question de l'évolution de la procédure pour l'adapter et l'améliorer, par une baisse de la protection des données personnelles. À cet égard, l'analyse consistant à discuter de la nature juridique et des missions des organismes pour décider de l'application de la procédure s'avère réductrice et risquée dans la mesure où elle se fonde sur une appréciation différente de la sensibilité de la donnée en fonction de celui qui la collecte. Au nom de quel principe protégerait-on davantage une donnée collectée par un médecin dans le cadre de l'administration des soins de celle collectée par un Registre du cancer ?
Toutefois, le CAH constate que cette interprétation large des textes peut être délicate à mettre en œuvre compte tenu des exigences posées par le décret du 4 janvier 2006 précité, fortement orienté pour des prestations d'hébergement de dossiers médicaux.
Une adaptation du décret et par conséquent du référentiel de constitution des dossiers de demande d'agrément sera indispensable afin que la constitution desdits dossiers soit à la portée de toutes les entités tenues d'être agréées.

C – LES PRESTATIONS « D'HÉBERGEMENT SEC »

Des prestataires proposent aujourd'hui à des établissements ou professionnels de santé des offres de *data center* sécurisés pour y stocker leurs machines, serveurs, baies, etc., contenant des données de santé à caractère personnel.
Les clients de ces hébergeurs déposent donc des données de santé à caractère personnel auprès d'un tiers chargé d'en assurer la sécurité physique et de contrôler les accès physiques au matériel contenant les données de santé.
Au vu de la définition large de la notion d'hébergement de données de santé retenue jusqu'à présent et de l'objectif poursuivi par les dispositions de l'article L.1111-8 qui visent à sécuriser les bases de données de santé, le CAH et la CNIL ont considéré que ces prestations entraient dans le champ d'application de l'article L.1111-8 précité.
Toutefois, il est nécessaire d'encadrer ces types de services.

Conformément aux dispositions de l'article L.1111-8 du code de la santé publique, lorsque la structure de soins ou le professionnel de santé héberge lui-même et par ses propres moyens les données de santé des patients qu'il prend en charge, il n'est pas soumis à la procédure d'agrément.

Toutefois, lorsque la structure de soins (ou le professionnel de santé, mais ce cas est assez rare) souhaite recourir à un prestataire tiers pour la location d'une salle blanche afin d'y déposer ses serveurs, qu'elle continue toutefois à exploiter et administrer elle-même, il a été jugé nécessaire d'encadrer le recours à ce prestataire tiers. En effet, ce prestataire est chargé de garantir la sécurité physique des équipements contenant des données de santé à caractère personnel et de proposer un environnement garantissant une conservation desdits équipements à l'état de l'art. Le Comité d'agrément des hébergeurs a donc considéré que ce type de prestation ne pouvait être proposé directement qu'à des professionnels, établissements de santé ou structures de soins pour l'hébergement des machines contenant les données de santé des patients qu'ils prennent en charge.
En effet, les prestations d'hébergement de données de santé de type « salle blanche » aujourd'hui agréées sont directement proposées à des professionnels, établissements de santé et plus largement des structures de soins.
Lorsque ces personnes physiques ou morales susvisées hébergent par leurs propres moyens les données de santé des patients qu'elles prennent en charge, elles ne sont pas soumises à la procédure d'agrément, mais restent toutefois redevables des formalités préalables au titre du respect de la loi Informatique et Libertés.
Dès lors, au regard de la finalité de la prestation offerte, l'hébergeur reporte sur son client la quasi-totalité des obligations du décret du 4 janvier 2006, celui-ci n'offrant que la sécurité physique du site d'hébergement, la disponibilité du réseau de télécommunication et quelques prestations dites « Hands and Eyes ». Les dossiers de demande d'agrément pour ce type de prestations ne décrivent donc pas les moyens logiques utilisés pour sécuriser les flux, réaliser les sauvegardes, tracer les accès des administrateurs, etc. (exigences de l'article R.1111-14 du code de la santé publique). Le contrat d'hébergement doit reprendre l'ensemble des exigences du décret reporté sur le client.

Le CAH a considéré que ce type de prestation ne devait être proposé qu'à des professionnels, établissements de santé ou structures de soins pour l'hébergement des machines contenant les données de santé des patients qu'ils prennent en charge et qu'ouvrir ce type de prestation à d'autres acteurs que ceux qui prennent en charge les patients pourrait conduire à une utilisation abusive de l'agrément. En effet, ne pas restreindre ce type de prestation pourrait permettre à des industriels ou des éditeurs de s'exonérer du dépôt d'un dossier de demande d'agrément en se prévalant de cet agrément, alors même qu'ils proposeraient à leurs clients finaux (professionnels de santé et structures de soins) une prestation de mise à disposition d'une plateforme technique d'hébergement d'applications contenant des données de santé à caractère personnel (avec fourniture ou non du logiciel métier).

Ce que doit renseigner un hébergeur qui souhaite déposer un dossier de demande d'agrément pour une prestation de mise à disposition de salle blanche

- Le contrat doit clairement préciser les types de client à qui la prestation peut être proposée : professionnels de santé, structures de soins.
- Le périmètre de la prestation doit être précis. Il convient d'indiquer si l'hébergeur réalise ou non des gestes de proximité, auquel cas cela doit être décrit dans le contrat.
- Toutes les exigences du décret du 4 janvier 2006 que l'hébergeur ne prend pas en charge lui-même doivent être reportées contractuellement sur le client et l'hébergeur doit accompagner ces reports d'un devoir de conseil (exemple : sécurité des flux, réalisation de sauvegardes, authentification forte des utilisateurs, gestion des évolutions, etc.).
- Pour la rédaction du modèle de contrat, le candidat peut s'aider du formulaire P6 et veiller à reporter contractuellement sur son client toutes les exigences qu'il ne prend pas en compte.

D - L'HÉBERGEMENT DE DONNÉES DE SANTÉ ÉCHANGÉES AU MOYEN D'UN SERVICE DE MESSAGERIE SÉCURISÉE DE SANTÉ

Un service de messagerie sécurisée de santé assure l'échange de données de santéà caractère personnel.

Un service de messagerie sécurisée de santé est un traitement de données à caractère personnel qui permet l'échange de données de santé entre plusieurs professionnels de santé ou personnes habilitées par la loi à échanger des données de santé à caractère personnel. Les échanges de données de santé doivent être réalisés dans le respect de la loi Informatique et Libertés et des dispositions du code de la santé publique, d'où la nécessité d'organiser la conservation des données de santé échangées conformément aux dispositions des articles L.1111-8 et R.1111-9 et suivants.

Pour les traitements de données personnelles qui sont nombreux à poursuivre la même finalité et présentent des caractéristiques communes, la CNIL peut élaborer des textes-cadres permettant aux responsables de traitement d'accomplir des formalités allégées.

S'agissant des traitements de messageries sécurisées de santé raccordés à l'espace de confiance, la CNIL a décidé, en application de l'article 25-II de la loi Informatique et Libertés que leur mise en œuvre pouvait être autorisée par une décision unique de la Commission. Dans ce cas, le responsable de chaque traitement adresse à la Commission un engagement de conformité de celui-ci aux conditions fixées par **l'autorisation unique**.

☒

Autorisation unique

** http://www.cnil.fr/documentation/deliberations/deliberation/delib/314/Délibération n° 2014-239 du 12 juin 2014.*

La CNIL a défini, en concertation avec l'ASIP Santé, les conditions que doit respecter tout responsable d'un traitement de messagerie sécurisée de santé.

Le responsable de traitement devra notamment s'assurer du respect des droits des personnes concernées par les données échangées, contrôler les destinataires des données et veiller à utiliser un outil de messagerie sécurisée de santé qui lui permette d'échanger les données de santé dans les conditions de sécurité définies dans l'autorisation unique.

L'autorisation unique impose ainsi que le service de messagerie utilisé :

— permette de garantir l'identité de l'émetteur et du destinataire d'un message en vérifiant leur appartenance à l'espace national de confiance santé social ;

— assure la sécurité des messages et des pièces jointes lors de leur transfert dans l'espace public ;

— assure la conservation sécurisée des messages et des pièces jointes : lorsque le responsable de traitement développe lui-même le service de messagerie sécurisée de santé utilisé par les utilisateurs finaux, et qu'il conserve par ses propres moyens les serveurs de messagerie sécurisée de santé, il est tenu de mettre en place les moyens techniques et organisationnels adéquats. Le responsable de traitement doit ainsi assurer la disponibilité, l'intégrité, la traçabilité et la sécurité physique et logique des messages et des pièces jointes qu'il conserve. Les moyens mis en œuvre doivent être conformes à l'état de l'art et adaptés à la finalité d'un service de messagerie sécurisée de santé. Ces moyens doivent correspondre aux mesures de sécurité retenues dans le cadre du plan de traitement des risques. Lorsque le responsable de traitement ne conserve pas par ses propres moyens les données de santé à caractère personnel échangées et collectées via un service de messagerie sécurisée de santé, il doit veiller à ce que les serveurs de messagerie soient conservés par un hébergeur agréé à cet effet, dans les conditions définies aux articles L.1111-8 et R.1111-9 et suivants du code de la santé publique. L'hébergeur ainsi agréé garantit la disponibilité, l'intégrité, la confidentialité et la traçabilité des données de santé.

Les agréments qui permettent d'héberger des services de messagerie sécurisée de santé

■ Soit l'hébergeur est agréé pour l'hébergement d'applications de type messagerie sécurisée de santé et prévoyant l'obligation pour le professionnel de santé d'utiliser un moyen d'authentification forte par carte CPS ou tout autre dispositif équivalent pour accéder aux données de santé.

■ Soit l'hébergeur est agréé pour une prestation dite « générique », lui permettant d'héberger des applications contenant des données de santé à caractère personnel et prévoyant l'obligation pour le professionnel de santé d'utiliser un moyen d'authentification forte par carte CPS ou tout autre dispositif équivalent pour accéder aux données de santé.

Dès lors qu'il satisfait à l'ensemble des exigences de l'autorisation unique, le responsable de traitement doit donc uniquement adresser à la CNIL un engagement de conformité à l'autorisation unique. Dans le cas contraire, il est tenu de procéder à une demande d'autorisation de traitement « classique ».

E – L'HÉBERGEMENT DE DONNÉES DE SANTÉ COLLECTÉES PAR LES ORGANISMES D'ASSURANCE MALADIE

Les organismes d'assurance maladie sont tenus de collecter des données dans le cadre du remboursement des frais de santé.

Des données relatives aux consultations, interventions, actes réalisés, taux de remboursement, etc. sont ainsi collectées. Ces données sont des données de santé à caractère personnel et doivent donc être conservées dans le respect des dispositions de la loi Informatique et Libertés et du code de la santé publique.
Les caisses d'assurance maladie conservent donc des données de santé recueillies à l'occasion d'activités de prévention, de diagnostic ou de soin, dont la conservation doit respecter les dispositions de l'article L.1111-8 du code de la santé publique.
La CNIL et le CAH se sont d'ores et déjà prononcés sur un dossier de demande d'agrément de l'association de protection sociale du bâtiment et des travaux publics (PRO BTP) qui conserve pour le compte de ses membres – instituts de prévoyance – les données de santé nécessaires au remboursement des frais de santé. Le ministre en charge de la santé a ainsi agréé l'association PRO BTP pour l'hébergement de données de santé à caractère personnel collectées à l'occasion de remboursements de frais de santé via le système de tiers payant Cleyris.

F – L'HÉBERGEMENT DE DONNÉES DE SANTÉ COLLECTÉES AU MOYEN D'OBJETS CONNECTÉS

L'émergence de la e-santé a fait naître de nouvelles pratiques, de nouvelles habitudes de « mesure de soi » (communément appelées « ***Quantified self*** ») par lesquelles le citoyen prend connaissance de certains paramètres relatifs à sa santé afin d'améliorer ses habitudes de vie. Ainsi, nous pouvons trouver dans le commerce de nombreux « objets connectés » qui calculent le nombre de pas, le nombre de calories dépensées, la tension, le poids etc. et envoient ces données sur un serveur afin que la personne puisse consulter ses données.
La frontière entre données de bien-être et données de santé est assez ténue, puisque ces premières peuvent donner des indications sur l'état de santé d'une personne. Doit-on ou non les considérer comme des données de santé à caractère personnel, dont la collecte, l'utilisation et la conservation sont soumises aux règles du code de la santé publique (référentiels de sécurité et d'interopérabilité, carte CPS ou dispositifs équivalents, hébergement de données de santé, etc.) ?
Dès lors que les données de bien-être sont uniquement utilisées par la personne concernée par les données pour améliorer ses habitudes quotidiennes, elles peuvent parfois être des données de santé, mais ne nécessitent pas d'encadrement supplémentaire à ce qu'impose d'ores et déjà la loi Informatique et Libertés.

La CNIL a publié des recommandations relatives au traitement des données collectées dans le cadre de service de *quantified self*.
Pour préserver le respect de leur vie privée, la CNIL recommande aux utilisateurs :
— d'utiliser, si possible, un pseudonyme pour partager les données ;

Quantified self
Voir *La lettre innovation et prospective de la CNIL*, n° 5, juillet 2013.

— de ne pas automatiser le partage des données vers d'autres services (notamment vers les réseaux sociaux) ;
— de ne publier les données qu'en direction de cercles de confiance ;
— d'effacer ou de récupérer les données lorsqu'un service n'est plus utilisé.
La CNIL met également en garde les utilisateurs sur la prolifération de leurs données via les réseaux sociaux et rappelle que la frontière peut être floue entre le médical et le simple suivi de son bien-être. Une donnée peut sembler anodine pour un utilisateur au moment où il la partage, mais receler beaucoup d'informations pour un spécialiste qui pourrait y avoir accès par la suite.

En revanche, dès lors que ces mêmes données sont utilisées dans le cadre de la prise en charge sanitaire de la personne concernée par un professionnel ou établissement de santé, leur traitement nécessite de respecter l'ensemble des dispositions du code de la santé publique qui encadrent leur utilisation, dont l'article L.1111-8 du code de la santé publique. Au surplus, l'ensemble des conditions qui définissent le « cercle de confiance de l'échange et du partage des données de santé » doit alors être respecté : identification et authentification des professionnels de santé et des patients, cadre national d'interopérabilité des systèmes d'information de santé (CI-SIS), procédure d'agrément pour l'hébergement de données de santé, politique générale de sécurité des systèmes d'information de santé.

Exemple

■ En reprenant l'exemple du glucomètre présenté au point C de la partie II *(cf. page 15)* : si, contrairement à ce qui est exposé au point II-C, le glucomètre est uniquement utilisé par la personne afin de contrôler sa glycémie et adapter elle-même ses habitudes alimentaires, sans qu'un professionnel de santé n'y ait accès, il s'agit là d'un service à valeur ajoutée proposé à la personne pour améliorer ses habitudes de vie et qui n'est donc pas soumis aux dispositions du code de la santé publique relatives à la protection des données de santé. Le service doit néanmoins respecter les dispositions de la loi Informatique et Libertés.

CONCLUSION

Au-delà des contrôles effectués par la CNIL et le CAH sur le respect des conditions posées par le décret du 4 janvier 2006, la chaîne de l'hébergement apparaît aujourd'hui longue et complexe. L'hébergeur n'assure pas toujours lui-même toutes les fonctions techniques nécessaires et s'appuie assez fréquemment sur des sous-traitants. À titre d'illustration, de nombreux hébergeurs recourent à des sous-traitants pour la gestion de sites de secours distants du site d'exploitation. Ce peut être le cas pour l'hébergement physique, pour lequel le candidat à l'hébergement peut faire appel à des fournisseurs de « salles blanches ».

De fait, le candidat à l'agrément n'occupe pas toujours la même position dans la chaîne de valeur. Parfois, il assure lui-même la gestion des applications de santé, mais dans certains cas, il assure seulement une fonction que l'on pourrait qualifier de « support » : des fournisseurs de puissance de calcul sans spécificité particulière, voire même des offreurs de salles blanches, se sont portés candidats.

Ce constat appelle dès lors deux questions : les industriels porteurs d'activités de support, très éloignés du destinataire final, sont-ils en mesure, même au travers de contrats et de leur devoir de conseil, de garantir le respect des obligations du décret vis-à-vis de l'utilisateur final ? Inversement, certaines de ces obligations, comme le recueil du consentement du patient, ne sont-elles pas dans tous les cas trop étrangères à l'activité d'hébergement pour en faire porter la responsabilité à l'hébergeur, alors que la prestation d'information réalisée pour le patient bénéficie dans l'immense majorité des cas d'une médiation par un professionnel de santé ?

Le Comité aura à cœur d'affiner sa doctrine à cet égard, et de la rendre transparente au travers de la communication institutionnelle de l'ASIP Santé et de la FAQ.

Jusqu'à présent, le CAH a adopté une interprétation large de l'article L.1111-8 du code de la santé publique à des fins de protection des données de santé des citoyens. Si cette position venait à changer, elle devrait être justifiée par des considérations qui ne remettent pas en cause le niveau de protection dû au citoyen et qui assurent à tous la même égalité de traitement.

Le Comité d'agrément a conscience de la complexité de la procédure d'agrément pour les industriels et a pu constater au fil des instructions des dossiers les limites de cette procédure qui est orientée pour des prestations d'hébergement de dossiers médicaux, alors même que l'esprit du texte vise à protéger toutes les données de santé à caractère personnel, recueillies ou produites à l'occasion d'activités de prévention, de diagnostic ou de soins.

Le CAH propose que les pouvoirs publics définissent plus clairement le périmètre de l'article L.1111-8 du code de la santé publique et souhaiterait que la procédure d'agrément (le décret 2006-6 du 4 janvier 2006) soit modifiée afin de pouvoir s'adapter à la finalité de la prestation d'hébergement présentée dans chaque dossier. Pour ce faire, il pourrait être intéressant de s'orienter vers une procédure de certification en s'inspirant de ce qui existe dans le domaine bancaire (certification PCIDSS -*Payment Card Industry Data Security Standard*).

Cette évolution de la procédure pourrait également conduire à supprimer la double instruction des dossiers par la CNIL, puis par le CAH, qui est redondante sur la quasi-totalité des points d'analyse. Le CAH pourrait ainsi conserver son rôle et la CNIL contrôlerait uniquement les responsables de traitement et pourrait multiplier les contrôles des hébergeurs agréés ou non.

Le Comité d'agrément souhaiterait ainsi que les pouvoirs publics mobilisent les moyens nécessaires pour mettre en place une procédure de contrôle des hébergeurs agréés, telle que prévue par l'article L.1111-8 du code de la santé publique. En effet, la procédure d'agrément est déclarative et aucun contrôle sur place n'est réalisé au moment de l'analyse des dossiers de demande d'agrément. Il semble important de pouvoir contrôler la mise en œuvre par les hébergeurs des éléments déclarés dans leur dossier. Ces contrôles compléteraient ainsi ceux réalisés par la CNIL au titre de la loi Informatique et Libertés.

Le Comité d'agrément constate que l'absence de contrôle des hébergeurs, qu'ils soient agréés ou non, peut laisser penser à certains prestataires de services et certains professionnels ou établissements de santé que le non-respect des dispositions de l'article L.1111-8 du code de la santé publique n'aurait pas d'impact majeur sur leurs activités respectives.

Au-delà des sanctions pénales prévues par les textes en cas de défaut d'agrément (articles L.1115-1 et L.1115-2 du code de la santé publique) et de possible mise en jeu de la responsabilité civile, voire même pénale du professionnel ou de la structure de soins qui externaliserait les données de santé de ses patients auprès d'un prestataire non agréé, force est de constater que la procédure d'agrément s'impose chez les acteurs des secteurs sanitaires et médico-sociaux, pas tant par les sanctions que par son caractère incontournable pour la sécurité des systèmes d'information aujourd'hui.

En outre, il convient de rappeler que cette procédure s'inscrit dans un ensemble plus large de référentiels et qu'indépendamment du respect de la procédure d'agrément, les professionnels de santé et structures de soins doivent respecter les conditions du « cercle de confiance de l'échange et du partage des données de santé » :
— les référentiels d'identification des acteurs de santé ;
— le cadre national d'interopérabilité des systèmes d'information de santé (CI-SIS) ;
— la politique générale de sécurité des systèmes d'information de santé qui comporte les référentiels d'authentification des professionnels de santé et des patients.

La procédure d'agrément pour l'hébergement de données de santé a permis de réguler et d'homogénéiser les prestations d'externalisation des données de santé en imposant un niveau de sécurité élevé.

Le Comité d'agrément constate que cette procédure a réussi à s'imposer dans le paysage de la e-santé compte tenu de sa finalité qui est et doit rester la protection des données de santé des citoyens.

Annexe I

Rappel du déroulement de la procédure d'agrément

L'ESSENTIEL

Toute personne physique ou morale qui conserve pour le compte d'un tiers des données de santé à caractère personnel recueillies à l'occasion d'activité de prévention de diagnostic ou de soins doit être agréée à cet effet.

L'agrément est délivré pour une durée de trois ans à l'issue d'une procédure qui fait intervenir la CNIL, le CAH et le ministre en charge de la santé et nécessite le dépôt d'un dossier de demande d'agrément qui doit définir la prestation objet de la demande d'agrément notamment au travers du contrat d'hébergement (pour plus de précisions, cf. point A) et les moyens de sécurité réellement mis en œuvre pour garantir la sécurité des données de santé dans le respect des droits des patients (pour plus de précisions, cf. point B).
À l'issue des trois ans, l'hébergeur doit déposer un dossier de demande de renouvellement d'agrément, qui doit lister les modifications apportées depuis le dossier initial, et un audit externe de sécurité, qui doit attester du respect effectif des exigences de sécurité posées par le décret « hébergeur » *(pour plus de précisions, cf. point C et Partie I du rapport d'activité).*

Toute personne physique ou morale qui souhaite proposer une prestation d'hébergement de données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic ou de soins doit être agréée à cet effet (article L.1111-8 du code de la santé publique)
L'agrément requis est délivré à l'issue d'une procédure strictement définie par le décret 2006-6 du 4 janvier 2006.

Le dossier

Le candidat doit constituer son dossier de demande d'agrément en veillant à apporter l'ensemble des informations suivantes exigées par le décret précité et traduites au travers d'un référentiel établi en concertation avec les industriels et la CNIL et composé de sept formulaires.

- **Formulaire P1 :** présentation du candidat et de sa situation financière.
- **Formulaire P2 :** présentation des sous-traitants. Le candidat doit joindre le contrat conclu avec le sous-traitant.
- **Formulaire P3 :** modèle de contrat d'hébergement. Ce contrat doit définir le périmètre de la prestation objet de la demande d'agrément. Cette prestation doit être présentée et encadrée dans le modèle de contrat d'hébergement.
- **Formulaire P4 :** description technique de la prestation d'hébergement, notamment au travers d'architectures techniques et fonctionnelles.
- **Formulaire P5 :** analyse de risques.
- **Formulaire P6 :** présentation de la politique de sécurité des systèmes d'information et des moyens techniques mis en œuvre pour garantir la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données de santé à caractère personnel.

Le dossier de demande d'agrément est tout d'abord instruit par la CNIL. La CNIL analyse les dossiers afin de s'assurer que les droits des personnes concernées par les données de santé sont garantis et que les moyens de sécurité mis en œuvre sont adaptés à la nature particulièrement sensible des données de santé.

Chaque dossier de demande d'agrément est présenté en séance plénière de la CNIL, puis la délibération (c'est-à-dire l'avis de la CNIL) est transmise au CAH.

Le CAH est un organe consultatif créé par le décret du 4 janvier 2006 précité. Le CAH est composé de personnalités qualifiées désignées par arrêté ministériel pour une durée de cinq ans, renouvelable une fois, qui exercent leur mission en toute indépendance (membres de l'IGAS, représentants d'associations compétentes dans le domaine de la santé, représentants des professions de santé, personnes compétentes dans les domaines de l'éthique et du droit, de la sécurité des systèmes d'information et dans le domaine économique et financier).

Compte tenu du nombre important de dossiers de demande d'agrément et du travail considérable que nécessite leur instruction, le secrétaire général des ministères chargés des Affaires sociales a confié à l'ASIP Santé la gestion du secrétariat du CAH et la pré-instruction des dossiers de demande d'agrément pour le compte du CAH.

Ainsi, avant présentation devant le Comité, les dossiers sont pré-instruits par l'ASIP Santé qui a créé à cet effet un comité d'instruction interne qui analyse les dossiers sous trois angles.

- **Un volet économique et financier** qui permet d'apprécier la solidité financière du candidat. Il convient de rappeler qu'une société nouvellement créée peut déposer un dossier de demande d'agrément et ne sera pas pénalisée sur ce point dès lors que son dossier démontre sa capacité à garantir la sécurité des données de santé hébergées.
- **Un volet éthique et juridique** qui consiste à analyser le contrat d'hébergement de données de santé, les relations avec les sous-traitants éventuels, le contrat du médecin de l'hébergeur, le respect des droits des personnes et, plus globalement, les modalités de proposition de la prestation d'hébergement de données de santé à caractère personnel.
- **Un volet sécurité et technique** qui analyse les moyens présentés par le candidat pour garantir la sécurité des données de santé (moyens techniques, organisationnels, analyse de risques, etc.).

Le comité d'instruction interne à l'ASIP Santé se réunit mensuellement afin de valider les pré-analyses des dossiers de demande d'agrément avant transmission aux membres du Comité d'agrément.
Un membre du Comité d'agrément est désigné rapporteur d'un dossier de demande d'agrément, analyse ce dossier et le présente en séance du Comité d'agrément. À l'issue de cette présentation, les membres débattent sur le dossier, puis procèdent au vote. Une majorité qualifiée de votes favorables est nécessaire pour que l'avis du Comité soit favorable. Les débats et les avis du CAH ne sont pas rendus publics. Les moyens adéquats ont donc été mis en œuvre afin de préserver leur confidentialité.
Les avis de la CNIL et du CAH sont ensuite transmis au ministre en charge de la santé, qui décide ou non d'agréer le candidat à l'agrément.

Le rapport annuel d'autoévaluation

Si le candidat est agréé, il s'engage à transmettre chaque année un rapport d'autoévaluation qui consiste à porter à la connaissance du ministre en charge de la santé toutes les modifications et évolutions apportées au dossier de demande d'agrément initial. Les modifications apportées ne peuvent modifier le périmètre de la prestation initialement agréée. En effet, une telle modification nécessiterait le dépôt d'un nouveau dossier de demande d'agrément et non simplement l'envoi d'une mise à jour dans le cadre d'un rapport annuel d'autoévaluation.
Les modifications apportées à ces dossiers sont analysées au regard de la prestation initialement agréée. À l'issue de l'instruction des rapports annuels d'autoévaluation, trois types de courriers sont adressés aux hébergeurs :
— soit les modifications apportées n'appellent aucune observation particulière et cela est mentionné au candidat ;
— soit les modifications apportées nécessitent des demandes de compléments d'information ou font apparaître des points d'attention : une demande de précision est alors adressée au candidat ;
— soit il apparaît que l'hébergeur a modifié substantiellement le périmètre de la prestation d'hébergement de données de santé et il est alors indiqué au candidat que les modifications apportées nécessitent le dépôt d'un nouveau dossier de demande d'agrément.

Le renouvellement de l'agrément

Enfin, au moins six mois avant la fin de la période d'agrément (trois ans), l'hébergeur doit adresser un dossier de demande de renouvellement d'agrément. Ce point est particulièrement développé dans la partie C du rapport.

Annexe 2

Arrêté de nomination des membres du Comité d'agrément

MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

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

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.

Arrêté du 5 février 2013 portant modification de l'arrêté du 14 juin 2011 fixant la composition du Comité d'agrément des hébergeurs de données de santé à caractère personnel.

Par arrêté de la ministre des Affaires sociales et de la Santé en date du 5 février 2013, les dispositions de l'arrêté du 14 juin 2011 fixant la composition du Comité d'agrément des hébergeurs de données de santé à caractère personnel sont modifiées comme suit:

Au lieu de: « et M. Jérôme GUÈDE, suppléant »,
Lire: « et M. Aurélien BESSON, suppléant ».

Annexe 3

Liste des hébergeurs agréés de données de santé à caractère personnel

(mise à jour : 9 juillet 2014)

Liste des hébergeurs agréés de données de santé à caractère personnel

Dans le cadre de la procédure d'agrément des hébergeurs de données de santé à caractère personnel précisée par le décret du 4 janvier 2006, 69 décisions d'agrément ont à ce jour été rendues, par le ministre en charge de la santé.

Il s'agit des sociétés ou organismes suivants :

■ **2CSI :** www.2csi.info
La société 2CSI est agréée pour l'hébergement de données de santé à caractère personnel gérées via ses progiciels fonctionnant sur son système d'information ERP Sano.

■ **AATLANTIDE :** www.aatlantide.com
La société Aatlantide est agréée pour une prestation d'hébergement de données de santé à caractère personnel gérées via son service Acteur.fr et ActeurCS.fr.

■ **Almérys SAS :** www.almerys.com
La société Almérys est agréée pour l'hébergement de données de santé à caractère personnel gérées par les applications Sesame RH et Teamlive.

■ **Almérys SAS :** www.almerys.com
La société Almérys est agréée pour une prestation d'hébergement de la solution logicielle « Système de gestion dossier patient informatisé (SGDPI) », dont elle est éditrice.

■ **Almérys SAS :** www.almerys.com
La société Almérys est agréée pour une prestation d'hébergement concernant la solution logicielle « Système de gestion de suivi et prévention santé (SGSPS) » dont elle est éditrice.

■ **Almérys SAS :** www.almerys.com
La société Almérys est agréée pour l'hébergement de données de santé à caractère personnel gérées via la solution logicielle « Serveur de prescriptions et de résultats d'examens (SPRE) ».

■ **Arrow ECS :** www.arrowecs.fr
La société Arrow ECS est agréée pour une prestation d'hébergement d'applications fournies par les clients et gérant des données de santé à caractère personnel collectées à des fins de suivi médical.

■ **Assistance publique des hôpitaux de Marseille (AP-HM) :** http://fr.ap-hm.fr/ap-hm
L'Assistance publique des hôpitaux de Marseille est agréée pour l'hébergement de données de santé à caractère personnel collectées via la solution e-Nadis.

■ **Avenir Télématique (ATE) :** www.ate.info
La société Avenir Télématique (ATE) est agréée pour l'hébergement de données de santé à caractère personnel gérées par les applications fournies par ses clients (« Service d'hébergement de données de santé à caractère personnel »).

■ **AZ NetWork :** http://aznetwork.eu
La société AZ Network est agréée pour une prestation d'hébergement d'applications fournies par les clients et gérant des données de santé à caractère personnel.

■ **BT :** http://home.bt.com
La société BT Service SA est agréée pour le service d'hébergement de la Messagerie sécurisé de santé (« MSSanté ») développée par l'ASIP Santé.

■ **Bull :** www.bull.fr
La société Bull est agréée pour l'hébergement de données de santé à caractère personnel via son offre « Cloud Santé Bull ».

■ **Carestream :** www.carestream.fr
La société Carestream est agréée pour une prestation d'hébergement de données de santé à caractère personnel gérées via la solution de traitement et de partage de données d'imagerie médicale « VCS » (*Vue for Cloud-Based Services*).

■ **Cegedim :** www.cegedim.fr
La société Cegedim est agréée pour l'hébergement de données de santé à caractère personnel gérées via le service d'hébergement HDS et la solution GRS Cegedim permettant la mise en partage d'informations médicales.

■ **Cegedim :** www.cegedim.fr
La société Cegedim est agréée pour une prestation d'hébergement de données de santé à caractère personnel collectées via les logiciels « monLogicielMedical.com » et « monSuiviPatient.com ».

■ **CERNER :** www.cerner.com
La société Cerner est agréée pour l'hébergement de données de santé à caractère personnel gérées via son progiciel Millennium.

■ **Cheops Technology :** www.cheops.fr
La société Cheops Technology est agréée pour l'hébergement d'applications fournies par ses clients et gérant des données de santé à caractère personnel collectées à des fins de suivi médical, via des offres d'hébergement dédié ou mutualisé.

■ **Chorégie :** www.choregie.fr
Le groupement d'intérêt économique Chorégie est agréé pour une prestation d'hébergement de données de santé à caractère personnel « Sauvegarde de second niveau ».

■ **Chorégie :** www.choregie.fr
Le groupement d'intérêt économique Chorégie est agréé pour l'hébergement d'applications confiées par les clients (membres du GIE) et gérant des données de santé à caractère personnel à des fins de suivi médical.

■ **CHU de Nantes :** www.chu-nantes.fr
Le CHU de Nantes est agréé pour une prestation d'hébergement d'applications fournies par les clients et gérant des données de santé à caractère personnel, ainsi que pour une prestation d'hébergement de serveurs contenant des données de santé à caractère personnel.

■ **CHU de Nice :** www.chu-nice.fr
Le CHU de Nice est agréé pour l'hébergement de données de santé à caractère personnel via l'application e-nadis.

■ **CHU de Nice :** www.chu-nice.fr
Le CHU de Nice est agréé pour l'hébergement de données de santé à caractère personnel gérées par l'application Calliope.

■ **CHU de Nice :** www.chu-nice.fr
Le CHU de Nice est agréé pour une prestation de mise à disposition, d'exploitation et de gestion d'une plateforme technique destinée à héberger des applications contenant des données de santé à caractère personnel, confiées par ses partenaires.

■ **CIS Valley :** www.cis-valley.fr
La société CIS Valley est agréée pour une prestation d'hébergement de données de santé à caractère personnel gérées par les applications fournies par les clients et collectées à des fins de suivi médical « Solution d'infogérance, d'hébergement et de secours ».

■ **DOCAPOST BPO :** www.docapost.com
La société DOCAPOST BPO est agréée en qualité d'hébergeur de données de santé à caractère personnel pour l'hébergement du dossier pharmaceutique, prévu à l'article L.1111-23 du code de la santé publique.

■ **EpiConcept :** www.epiconcept.fr
La société EpiConcept est agréée pour l'hébergement de la plateforme applicative Voozanoo qui propose des services en ligne de gestion de dossiers médicaux et de surveillance sanitaire.

■ **GCS EMOSIST-FC :** www.emosist.fr
Le groupement de coopération sanitaire EMOSIST-FC est agréé pour l'hébergement d'applications et de données de santé à caractère personnel du GCS EMOSIST-FC, pour son service Dossier médical partagé de Franche-Comté.

■ **GCS SIS de Martinique :** www.sante-martinique.fr
Le groupement de coopération sanitaire système d'information de santé de Martinique (GCS SISM) est agréé pour l'hébergement des applications et données de santé à caractère personnel gérées par la Plateforme régionale de santé de Martinique (infrastructure matérielle et logicielle) mise à la disposition de ses membres.

■ **GCS Télésanté Lorraine :** www.sante-lorraine.fr
Le groupement de coopération sanitaire télésanté Lorraine est agréé pour l'hébergement de données de santé à caractère personnel collectées via l'outil T-Lor, outil de partage de données de santé et d'images médicales dans le cadre d'activités de télémédecine.

■ **GIP MiPih :** www.mipih.fr
Le GIP Midi Picardie Informatique Hospitalière est agréé pour l'hébergement de données de santé à caractère personnel collectées via le progiciel « Pastel » dont il est éditeur.

■ **GIP MiPih :** www.mipih.fr
Le GIP Midi Picardie Informatique Hospitalière est agréé pour une prestation d'hébergement de données de santé à caractère personnel gérées par des applications fournies par les clients.

■ **GMI Expert :** www.mes-sauvegardes-de-sante.com
La société GMI Expert est agréée pour une prestation d'hébergement de sauvegardes de données de santé proposée à des professionnels ou établissements de santé dénommée « http://www.mes-sauvegardes-de-sante.com/ ».

■ **GRITA SAS :** http://www.grita.fr
La société Grita SAS est agréée pour l'hébergement de données de santé à caractère personnel collectées par les applications de ses clients via son service « Host Medical Externalisation ».

■ **H2AD :** www.h2ad.net
La société H2AD est agréée pour l'hébergement de données de santé à caractère personnel collectée via la solution « Dossier patient participatif » (D2P), service Web de mise en partage de données de santé.

■ **HCL :** www.chu-lyon.fr/web
Les HCL (Hospices civils de Lyon) sont agréés pour l'hébergement d'applications gérant des données de santé à caractère personnel.

■ **IBO :** www.ibo.fr
La société IBO est agréée pour une prestation d'hébergement d'applications fournies par les clients et gérant des données de santé à caractère personnel.

■ **IDS :** www.ids-assistance.com
La société IDS (Informatique de sécurité) est agréée pour l'hébergement de données de santé à caractère personnel gérées par les applications métier de ses clients permettant la mise en partage de données de santé à caractère personnel et pour l'application Pardosan fournie par IDS.

■ **International Cross Talk :** www.group-ict.com
La société International Cross Talk (ICT) est agréée pour l'hébergement de données de santé à caractère personnel gérées par ses applications Chorus et Chrysalide.

■ **I-Invest :** www.i-invest.net
La société I-Invest est agréée pour l'hébergement de la prestation dénommée « [in] Hosting-Santé » dédiée exclusivement aux établissements de santé.

■ **Interxion :** www.interxion.com/fr
La société Interxion est agréée pour une prestation de mise à disposition de salle blanche (salle privative, cage privative ou baie en espace partagé), ainsi que la fourniture de l'alimentation électrique et des réseaux de télécommunication, pour accueillir les équipements des clients et les applications contenant des données de santé à caractère personnel. Cette prestation est proposée directement aux responsables de traitement de données de santé à caractère personnel collectées à l'occasion de leurs activités de prévention de diagnostic ou de soins et qui administrent par leurs propres moyens leurs équipements.

■ **Le Réseau Santé Social :** www.cgm.com/fr
Le Réseau Santé Social (CompuGroup Medical France) est agréé pour l'offre « Fortidata Hébergement sécurisée », service d'hébergement sécurisé pour les applications, les plateformes applicatives dans le domaine médical, ainsi que les données de santé associées.

■ **Le Réseau Santé Social :** www.cgm.com/fr
Le Réseau Santé Social (CompuGroup Medical France) est agréé pour la prestation d'hébergement de données de santé à caractère personnel « Fortidata Sauvegarde en Ligne (SEL) », service de sauvegarde en ligne de données de santé collectées par des professionnels de santé.

■ **Navaho :** www.navaho.fr
La société Navaho est agréée pour une prestation d'hébergement « Solution logicielle Navaho Santé Archivage », service d'archivage de données de santé à caractère personnel.

■ **NetPlus :** www.netplus.fr
La société NetPlus est agréée pour une prestation d'hébergement d'applications fournies par le client et contenant des données de santé à caractère personnel collectées à des fins de suivi médical.

■ **NCS :** www.ncs.fr
La société NCS est agréée pour la mise à disposition d'infrastructures techniques, informatiques et réseaux permettant de faire fonctionner les applications et les données de santé associées d'établissements de santé.

■ **NUMERGY :** www.numergy.com
La société Numergy est agréée pour une prestation d'hébergement de données de santé à caractère personnel au travers de l'offre « Cloud Santé » qui consiste à mettre à disposition de ses clients une plateforme technique d'hébergement pour accueillir des applications gérant des données de santé à caractère personnel.

■ **ORANGE :** www.orange-business.com/fr
La société Orange est agréée pour la prestation d'hébergement de données de santé à caractère personnel via son service « Solution Hébergement Santé – Infogérance d'applications ».

■ **ORANGE BUSINESS :** www.orange-business.com/fr
La société Orange Business est agréée pour la prestation d'hébergement « Services d'imageries médicales partagées », pour le compte du Groupement de coopération sanitaire pour le développement des systèmes d'information en santé partagés en Île-de-France (GCS D-SISIF).

■ **ORANGE BUSINESS :** www.orange-business.com/fr
La société Orange Business est agréée pour un service d'hébergement d'applications fournies par les clients et gérant des données de santé à caractère personnel « Plateforme Santé – OS managé et Logiciel d'infrastructure managé ».

■ **Pacesetter:** www.sjm.com
La société Pacesetter est agréée pour l'hébergement de données de santé à caractère personnel gérées par le système Merlin.net

■ **Pharmagest:** www.pharmagest.com
La société Pharmagest est agréée pour l'hébergement de données de santé à caractère personnel pour une prestation d'hébergement de sauvegardes externalisées de données de santé.

■ **Pharmagest:** www.pharmagest.com
La société Pharmagest est agréée pour une prestation d'hébergement d'applications gérées et administrées par le client et contenant des données de santé à caractère personnel collectées dans le cadre d'activités de télémédecine « Service TELE100T ».

■ **Pharmagest:** www.pharmagest.com
La société Pharmagest est agréée pour le service « TELE100T- APS (Accès patient sécurisé) », prestation d'hébergement d'applications gérées et administrées par le client et contenant des données de santé à caractère personnel collectées à des fins de suivi médical.

■ **Pictime:** www.pictime-groupe.com/
La société Pictime-Coreye est agréée pour un service d'hébergement de données de santé à caractère personnel gérées par les applications de ses clients, via son offre « Silver Santé ».

■ **PRO BTP:** www.probtp.com
L'association de protection sociale du bâtiment et des travaux publics (PRO BTP) est agréée pour l'hébergement de données de santé à caractère personnel collectées à l'occasion de remboursements de frais de santé via le système de tiers payant Cleyris. Cette prestation est offerte aux membres de l'association.

■ **Proginov:** www.proginov.com
La société Proginov est agréée pour une prestation d'hébergement d'applications en mode Saas, fournies et maintenues par le client et gérant des données de santé à caractère personnel produites par des services de santé au travail.

■ **Prosodie Capgemini:** www.prosodie.fr
La société Prosodie Capgemini est agréée pour l'hébergement de données de santé à caractère personnel gérées par les applications fournies par ses clients et utilisées à des fins de suivi médical.

■ **SANTEOS:** www.santeos.com
La société Santéos est agréée pour l'hébergement d'applications métiers fournies par les clients, gérant des données de santé à caractère personnel collectées à des fins de suivi médical.

■ **SANTEOS DMPv1 :** www.santeos.com
Le groupement Santéos, Atos Worldline, Extelia est agréé pour l'hébergement du dossier médical personnel.

■ **SFR :** www.sfrbusinessteam.fr/sante
La Société française du radiotéléphone (SFR) est agréée pour l'hébergement de plateformes gérant des données de santé à caractère personnel via son offre « Services managés Santé » (les plateformes managées peuvent reposer sur des infrastrucutres dédiées aux clients et les offres Cloud Computing de SFR).

■ **SIGEMS:** www.sigems.fr
La société Sigems Data Center est agréée en qualité d'hébergeur de données de santé à caractère personnel. Cet agrément vaut pour la prestation d'hébergement avec l'utilisation des logiciels Sigems et la prestation d'hébergement simple.

■ **Sigma Informatique:** www.sigma.fr
La société Sigma Informatique est agréée pour son offre « Infogérance d'un système d'information incluant l'hébergement de données de santé à caractère personnel gérées par les applications fournies par les clients et utilisées à des fins de suivi médical ».

■ **Softway Medical Services:** www.softway-medical.fr
La société Softway Medical Services est agréée pour l'hébergement d'applications gérant des données de santé à caractère personnel utilisées à des fins de suivi médical.

■ **Solware Life:** www.solware.fr/life
La société Solware Life est agréée pour l'hébergement de données de santé à caractère personnel gérées par le progiciel « easy-suite » dont elle est éditrice.

■ **Sorin CRM:** www.sorin.com
La société Sorin CRM est agréée pour l'hébergement de données de santé à caractère personnel collectées via le service « Remote Monitoring System » (RMS), service associé à la délivrance de défibrillateurs cardiaques.

■ **Syndicat interhospitalier d'informatique hospitalière du Nord-Pas-de-Calais :**
www.siih5962.fr
Le Syndicat interhospitalier d'informatique hospitalière du Nord-Pas-de-Calais (SiiH) est agréé pour l'hébergement d'applications fournies par les clients et gérant des données de santé à caractère personnel.

■ **Syndicat interhospitalier d'informatique hospitalière du Nord-Pas-de-Calais :**
www.siih5962.fr
Le Syndicat interhospitalier d'informatique hospitalière du Nord-Pas-de-Calais (SiiH) est agréé pour une prestation d'hébergement de données de santé à caractère personnel via une plateforme régionale d'échange d'images médicales et de documents associés.

■ **Syndicat interhospitalier de Bretagne :**
www.sib.fr
Le Syndicat interhospitalier de Bretagne (SIB) est agréé pour l'hébergement de données de santé à caractère personnel gérées par des plateformes de télésanté ou des applications informatiques confiées par ses adhérents ou clients.

■ **Syndicat interhospitalier du Limousin :**
www.silpc.fr
Le Syndicat interhospitalier du Limousin (SIL) est agréé pour un service d'hébergement de données de santé à caractère personnel gérées par des applications métiers fournies par leurs adhérents et gérant des données de santé à caractère personnel, ainsi que pour un service de stockage de données de santé à caractère personnel dans le cadre de plans de continuité et de reprise d'activité (PCA/PRA).

Annexe 4

Foire aux questions sur le référentiel de constitution des dossiers de demande d'agrément

Cette FAQ est régulièrement mise à jour sur le site de l'ASIP Santé pour répondre, au fil de l'eau, aux questions posées par les demandeurs d'agrément.

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 (http://esante.gouv.fr/sites/default/files/HDS_papier.pdf).

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.

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 services d'hébergement, n'est autorisée.

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 vingt 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.

FAQ
http://esante.gouv.fr/services/referentiels/securite/hebergement-faq

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 (système d'information de santé) 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.

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 type 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.

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 services qu'il soit agréé comme hébergeur ?
Dans le cadre d'un appel d'offres pour un système d'information nécessitant un volet hébergement de données de santé à caractère personnel, le titulaire du marché est soumis à la procédure d'agrément prévue par l'article L.1111-8 du CSP et son décret d'application n° 2006-6 du 4 janvier 2006.
Aussi, le titulaire du marché doit obtenir l'agrément avant l'hébergement des premières données de santé personnelles « réelles » (par exemple, la mise en exploitation de l'applicatif de gestion et d'hébergement de données de santé à caractère personnel).
L'agrément est délivré pour une durée de trois ans renouvelable, après dépôt d'une demande déposée au plus tard six mois avant le terme de la période d'agrément.
Si le titulaire du marché perd son agrément (retrait ou non renouvellement) en cours d'exécution du marché, le marché devra être résilié.

Comment se positionnent les traitements de contrôle d'accès aux données vis-à-vis de la procédure d'agrément ?
Le prestataire de services 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 le traitement de contrôle d'accès complémentaire est assuré par l'hébergeur).

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 traitement 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 trouve 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 font la différenciation et la mise en concurrence des offres des hébergeurs agréés.

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.

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.

À partir de quelle durée de conservation des données de santé à caractère personnel un prestataire de services 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 l'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.

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'étendue 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.

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'île 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 États-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.

Quel est le statut du « médecin de l'hébergeur » ?
L'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. À 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 services dès lors qu'il existe des clauses d'interdiction d'exercice d'activités incompatibles : médecin des assurances ou médecin du travail, par exemple.

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 leur 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.

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 clé 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.

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 en charge 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 4e trimestre de l'année 2010.

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.

Quelles sont les clauses à insérer dans le contrat de « médecin de l'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.

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.

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

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

■ **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 par 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 logiciels 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.

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 (cf. question p. 52, 1re col.) 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.

Quels éléments doit comporter l'audit externe qu'est tenu de réaliser tout hébergeur en cas de demande de renouvellement de son agrément ?

En cas de demande de renouvellement de son agrément, l'hébergeur doit adresser un dossier devant contenir les informations financières mises à jour, les moyens mis en œuvre pour prendre en compte les recommandations émises par le ministre en charge de la santé au moment de l'agrément initial, la liste des modifications intervenues depuis la dernière demande d'agrément et les résultats d'un audit externe.

Cet audit externe est réalisé aux frais de l'hébergeur et doit attester de la mise en œuvre de la politique de confidentialité et de sécurité mentionnée à l'article R.1111-14 du code de la santé publique.

Le prestataire d'audit est au libre choix de l'hébergeur, qui pourra utilement se référer au référentiel de qualification publié par l'ANSSI, notamment dans ses volets audit d'architecture, audit de configuration et audit organisationnel et physique (http://www.ssi.gouv.fr/fr/menu/actualites/publication-du-referentiel-d-exigences-applicable-aux-prestataires-d-audit-de.html).

Le périmètre de l'audit doit couvrir :

■ la conformité des moyens mis en œuvre par l'hébergeur au regard de son dossier d'agrément et des rapports d'autoévaluation subséquents ;

■ la conformité des moyens mis en œuvre au regard des exigences du décret en tenant compte des évolutions réglementaires et de l'état de l'art depuis son dossier initial ;

■ la prise en compte des éventuelles recommandations qui lui auraient été notifiées lors de son agrément initial et des rapports d'autoévaluation.

CONFORMITÉ DES MOYENS AUX ÉLÉMENTS DU DOSSIER D'AGRÉMENT

L'audit doit vérifier que les moyens techniques, les processus pour garantir la sécurité et confidentialité des données de santé et les reports contractuels de certaines exigences sur le client ou d'éventuels sous-traitants, présentés dans le dossier de demande d'agrément initial et les rapports d'autoévaluation, sont effectivement mis en œuvre.

CONFORMITÉ DES MOYENS AU REGARD DES EXIGENCES DU DÉCRET ET DES ÉVOLUTIONS DE L'ÉTAT DE L'ART

L'audit doit assurer que le dossier de demande de renouvellement reste conforme aux exigences du décret et tient compte des évolutions du cadre juridique et de l'état de l'art intervenues depuis son agrément initial.

PRISE EN COMPTE DES RECOMMANDATIONS

L'audit doit également prendre en compte les recommandations majeures qui accompagnaient la décision d'agrément et indiquer ce qui a ou non été mis en place par l'hébergeur pour les respecter.
Les recommandations émises par le ministre en charge de la santé au moment de l'agrément initial ne sont pas exhaustives et un certain nombre d'autres points d'attention peuvent subsister. Il convient de rappeler aux hébergeurs que le courrier de notification de décision favorable d'agrément précise que les services de l'ASIP Santé (qui assure le secrétariat du CAH et la pré-instruction des dossiers de demande d'agrément pour le compte du CAH) se tiennent à la disposition des candidats pour leur apporter toute information complémentaire. L'ensemble des points d'attention, même mineurs, peut donc être transmis à l'hébergeur si celui-ci en fait la demande et ce, dans une perspective d'amélioration de son service.

L'audit externe doit vérifier la mise en œuvre des points précités. À titre d'exemple, au travers d'une interview, l'auditeur pourrait vérifier si le médecin hébergeur est impliqué dans la gestion des incidents tel que cela pourrait être décrit dans ses missions ; en visitant le site d'un client de l'hébergeur, l'auditeur pourrait apprécier la mise en œuvre par le client de ses obligations définies dans le contrat d'hébergement.

Les résultats de l'audit permettront à l'hébergeur d'améliorer ses processus, de renforcer son devoir de conseil et de planifier un cycle d'amélioration de son service d'hébergement. Ce cycle d'amélioration doit traiter les remarques relevant de la conformité au dossier ou de la prise en compte des recommandations. Pour celles traitant des évolutions de l'état de l'art, l'hébergeur peut soit les intégrer à son plan d'actions, soit présenter avec son dossier de renouvellement un argumentaire explicitant en quoi il les considère comme excessives à ce jour, auquel cas le Comité d'agrément statuera par l'expression de nouvelles recommandations.

L'audit externe ne doit pas dater de plus de six mois avant le dépôt du dossier de demande de renouvellement.

Afin d'aider les hébergeurs à conduire l'audit externe, l'ASIP Santé propose un exemple de scénario **d'audit** portant sur la conformité des moyens techniques mis en œuvre par l'hébergeur, aux exigences du décret 2006-6 du 4 janvier 2006.

Ce document constitue un simple canevas qui répertorie les exigences énoncées dans le formulaire P6 et prises en compte par l'hébergeur lui-même.

Si l'auditeur utilise ce modèle, il est tenu de le compléter de l'ensemble des points exposés précédemment.

Dans quelles conditions est-il possible d'héberger un service de messagerie sécurisée de santé (MSSanté) ?

Dans la mesure où un service de messagerie sécurisée de santé assure l'échange de données de santé à caractère personnel, l'opérateur qui offre le service de messagerie doit également organiser la conservation des données de santé échangées par les utilisateurs de son service. Cette conservation doit être réalisée dans le respect des dispositions de l'article L.1111-8 du code de la santé publique et du décret 2006-6 du 4 janvier 2006 relatives à l'hébergement de données de santé à caractère personnel.

Selon les cas, l'hébergement des données de santé échangées via le service de messagerie sécurisée de santé peut être réalisé par l'opérateur lui-même ou par un prestataire tiers choisi par l'opérateur.

☒
Audit
http://esante.gouv.fr/sites/default/files/HDS-Exemple-Audit_de_conformite-Securite_et_Technique_v1_0.pdf

En tout état de cause, pour pouvoir héberger un service de messagerie sécurisée de santé, l'hébergeur (opérateur ou prestataire de l'opérateur) doit être titulaire d'un agrément couvrant une telle prestation :

■ **soit l'hébergeur est agréé pour l'hébergement d'applications** de type messagerie sécurisée de santé et prévoyant l'obligation pour le professionnel de santé d'utiliser un moyen d'authentification forte par carte CPS ou tout autre dispositif équivalent pour accéder aux données de santé ;

■ **soit l'hébergeur est agréé pour une prestation dite « générique »** lui permettant d'héberger des applications contenant des données de santé à caractère personnel et prévoyant l'obligation pour le professionnel de santé d'utiliser un moyen d'authentification forte par carte CPS ou tout autre dispositif équivalent pour accéder aux données de santé.

Que dois-je décrire dans mon dossier de demande d'agrément pour pouvoir héberger des applications prévoyant un accès direct du patient à l'application ?

Au regard du caractère sensible des données de santé à caractère personnel, l'accès de tout acteur aux données de santé doit être réalisé de façon sécurisée (article L.1110-4 du code de la santé publique qui dispose que le patient a droit au respect de sa vie privée et du secret des informations la concernant).

Le dossier de demande d'agrément doit décrire les modalités d'identification et d'authentification du patient.

1- IDENTIFICATION

Le dossier de demande d'agrément doit préciser les moyens mis en œuvre pour réaliser l'enrôlement du patient.
Les procédés suivis doivent notamment assurer l'attribution du bon identifiant au bon patient afin d'éviter les doublons et les risques de collision entre des dossiers de différents patients.

Lorsque l'hébergeur n'est pas en lien direct avec le patient, il doit clairement définir les principes que s'engage à respecter son client afin de garantir l'identification du patient.

2- AUTHENTIFICATION

Il est impératif d'utiliser un moyen d'authentification forte afin de préserver la sécurité des accès.
Plusieurs moyens d'authentification forte peuvent être mis en œuvre par l'hébergeur ou son client.

À titre d'exemples, voici quelques moyens qui peuvent être retenus.

■ **Utilisation d'un identifiant/passe associé à un mot de passe à usage unique (OTP = *One Time Password*) envoyé par mail ou SMS.**
Le dossier de demande d'agrément doit préciser :
— qui délivre le mot de passe au patient et par quel procédé (le mot de passe doit être personnalisé par le patient lors de la première connexion à l'application) ;
— qui recueille les informations relatives au canal de transmission de l'OTP (adresse e-mail ou numéro de téléphone mobile).

■ **Utilisation d'un certificat électronique de type carte à puce**
Le dossier de demande d'agrément doit préciser :
— les moyens de protection du certificat (code PIN, biométrie, etc.) ;
— qui délivre le certificat au patient et comment.

Lorsque l'hébergeur n'est pas en lien direct avec le patient, il doit clairement définir les principes que s'engage à respecter son client afin de garantir l'authentification forte du patient.

L'ASIP Santé assure le secrétariat du Comité
d'agrément des hébergeurs de données de santé.

ASIP Santé
9, rue Georges Pitard
75015 PARIS
Tél. : 01 58 45 32 50

esante.gouv.fr

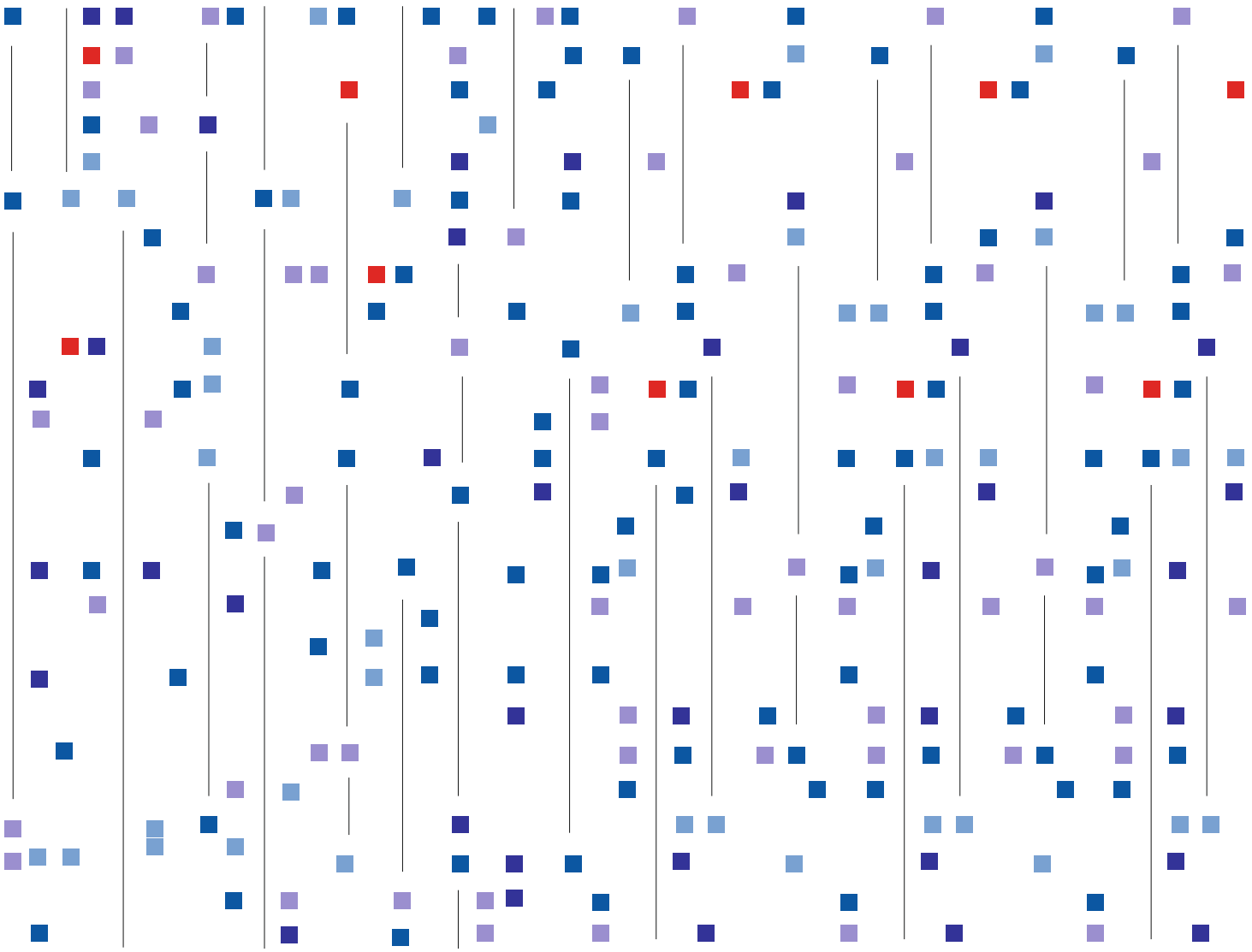
asipsanté

AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

L'ASIP Santé assure le secrétariat général du Comité d'agrément des hébergeurs de données de santé

ASIP Santé
9, rue Georges Pitard
75015 PARIS
Tél. : 01 58 45 32 50

esante.gouv.fr



Réalisation : Direction de la communication - BABEL – Septembre 2014