1 – Questions fréquentes

QUELS DROITS POUR LES PERSONNES CONCERNEES PAR LES DONNEES DE SANTE HEBERGEES ?

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*. [...] ».

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.

Une seconde dérogation permet à un établissement de santé qui décide désormais de faire héberger ses données par un hébergeur (alors que jusqu'à présent il les conservait dans ses murs) de ne pas solliciter le consentement de ses patients.

En tout état de cause, le patient dispose, 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'accès, d'opposition et de rectification.

LA PROCEDURE D'AGREMENT S'APPLIQUE-T-ELLE AUX ETABLISSEMENTS DE SANTE ?

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

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

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

UNE SOCIETE EST-ELLE AGREEE POUR L'ENSEMBLE DE SES ACTIVITES ?

Non. L'agrément ne permet pas de couvrir toutes les activités d'hébergement. Le candidat peut toutefois déposer un dossier de demande d'agrément intégrant plusieurs types de prestations de service d'hébergement de données de santé qu'il propose sur le marché dès lors que le modèle de contrat proposé permet de répondre aux exigences du décret. On parle alors de prestation « générique ». Sinon, un dossier de demande d'agrément doit être présenté pour chaque type de prestation d'hébergement.

Par type de prestation d'hébergement il faut entendre « modèle de contrat » différent, adapté à la typologie des clients de l'hébergeur.

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 SYSTEME D'INFORMATION NECESSITANT UN VOLET HEBERGEMENT DE DONNEES DE SANTE A CARACTERE PERSONNEL, A QUEL MOMENT FAUT-IL EXIGER DE MON PRESTATAIRE DE SERVICE QU'IL SOIT AGREE COMME HEBERGEUR ?

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 L1111-8 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 » (ie. 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.

A PARTIR DE QUELLE DUREE DE CONSERVATION DES DONNEES DE SANTE A CARACTERE PERSONNEL UN PRESTATAIRE DE SERVICE EST-IL CONSIDERE COMME HEBERGEUR ?

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

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

QUELLE DISTINCTION PEUT-ON FAIRE ENTRE ANONYMISATION ET CHIFFREMENT DES DONNEES DE SANTE ?

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

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

LES DONNEES DE SANTE DOIVENT-ELLES NECESSAIREMENT ETRE HEBERGEES SUR LE TERRITOIRE FRANÇAIS ?

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

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

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

- La Commission européenne a reconnu comme présentant un niveau de protection adéquat, les pays suivants : Canada, Suisse, Argentine, territoires de Guernesey, de Jersey et de l'Isle de Man.

- Les Biding Corporate Rules (BCR) ou règles internes d'entreprises : règles adoptées au sein d'un groupe multinational. Les BCR doivent revêtir un caractère contraignant et être respectées par les filiales du groupe.

- Les Clauses Contractuelles Types sont des modèles de clauses contractuelles adoptées par la Commission européenne permettant d'encadrer les transferts de données à caractère personnel.

- Le Safe Harbor concerne les entreprises situées aux Etats-Unis. Le Safe Harbor est un ensemble de principes de protection des données personnelles négociées par les autorités américaines et la Commission européenne en 2001. Les entreprises adhérentes au Safe Harbor doivent se conformer aux exigences de protection des données et assurent ainsi un niveau de protection adéquat.

EN MATIERE D'ANALYSE DE RISQUES EST-IL UTILE DE SE REFERER A LA NORME 27005 ?

Lors de la concertation qui a précédé la relance de la procédure d'agrément des hébergeurs en 2009, 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.

PUIS-JE HEBERGER DES DONNEES DE SANTE A CARACTERE 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 et que d'autre part, l'hébergement au sein de cette infrastructure de type Cloud computing réponde à toutes les exigences de sécurité du décret hébergeur.

QUE DOIS-JE DECRIRE DANS MON DOSSIER DE DEMANDE D'AGREMENT POUR POUVOIR HEBERGER DES APPLICATIONS PREVOYANT UN ACCES DIRECT DU PATIENT A 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 collisions 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 préserver la sécurité des accès.

Plusieurs moyens d'authentification forte peuvent être mis en œuvre par l'hébergeur ou son client.

A titre d'exemple, voici quelques moyens qui peuvent être retenus.

1- Utilisation d'un identifiant / mot de passe associés 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 mail ou numéro de téléphone mobile) ?

2- 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.

2 – L'audit externe

QUELS ELEMENTS DOIT COMPORTER L'AUDIT EXTERNE QU'EST TENU DE REALISER TOUT HEBERGEUR EN CAS DE DEMANDE DE RENOUVELLEMENT DE SON AGREMENT ?

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 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'auto évaluation, sont effectivement mis en œuvre.

- La 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.

- La 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, peuvent 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. A titre d'exemples, 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.

3 – MSSanté

DANS QUELLES CONDITIONS EST-IL POSSIBLE D'HEBERGER UN SERVICE DE MESSAGERIE SECURISEE DE SANTE (MSSANTE) ?

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**.

En tout état de cause, pour pouvoir héberger un service de messageries sécurisées 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 types messagerie sécurisées 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.