Cet article est paru initialement dans la Revue Lamy Droit de l'Immatériel, janvier 2015, n°111

Pour citer cet article : Lorraine Maisnier-Boché, « *Hébergement des données de santé : bilan et perspectives de réforme* », Revue Lamy Droit de l'Immatériel, 2015/111, pp.37-43.

HEBERGEMENT DES DONNEES DE SANTE : BILAN ET PERSPECTIVES DE REFORME

Lorraine Maisnier-Boché
Avocat au barreau de Paris / CIPP/E
Chargée d'enseignement auprès de l'Université Paris II Panthéon-Sorbonne

Cinq ans après les premiers agréments accordés aux hébergeurs de données de santé, le Comité d'agrément des hébergeurs (le « CAH ») vient de rendre son deuxième rapport d'activité, concernant les années 2012 et 2013[1]. Le précédent rapport du CAH datant de l'année 2011, ce nouveau rapport était très attendu.

Ce régime, créé par la loi du 4 mars 2002[2], souffre aujourd'hui de l'ancienneté et du laconisme de ses dispositions fondatrices[3]. Un décret d'application[4], le « décret hébergeur », est venu préciser ces dispositions sans toutefois aborder certains aspects essentiels de la mise en œuvre pratique de l'activité d'hébergeur agréé, comme par exemple le statut du médecin de l'hébergeur. Les particularités du domaine de la santé, n'ont pas été expressément prises en compte, tout particulièrement concernant l'accès aux données.

Parallèlement, le secteur de la santé numérique a connu une croissance exponentielle, que ce soit dans le cadre de la télémédecine, de la dématérialisation, de l'émergence des applications de suivi personnel et de façon générale, de ce qu'on appelle désormais la e-santé et la m-santé. Le régime de l'agrément hébergeur de données de santé a ainsi pris une importance considérable et a suscité un nombre croissant de questionnements.

A ce titre, la transformation en 2009 du Groupement d'Intérêt Public en charge du Dossier Médical Personnel (le « GIP-DMP ») en Agence des Systèmes d'Information Partagés de santé (« ASIP Santé ») a permis aux acteurs de la e-santé d'obtenir des lignes directrices bienvenues sur les points laissés en suspens par le décret hébergeur. En effet, l'ASIP Santé assure le secrétariat du CAH et assume dans les faits des missions rappelant celles d'un régulateur. La doctrine de l'ASIP Santé constitue aujourd'hui l'un des piliers de la mise en place concrète des projets dans la e-santé.

---

[1] Rapport d'activité 2012-2013 du Comité d'agrément des hébergeurs de données de santé, <http://esante.gouv.fr/sites/default/files/asip_cah_brochure_ra_2012-2013.pdf>

[2] Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé

[3] Article L.1111-8 du Code de la santé publique

[4] Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel

Il n'en demeure pas moins que depuis 2011, peu d'informations sur la doctrine ou sur les avis du CAH ont été rendues publiques. L'absence de publication, même partielle, des avis du CAH et de la Commission Nationale de l'Informatique et des Libertés (la « CNIL »), sur lesquels le ministre en charge de la Santé rend sa décision d'agrément, prive le secteur d'une précieuse source d'informations.

Dans ce contexte, le rapport du CAH fournit ainsi un retour d'expérience très attendu. Plus de 70 dossiers ont été reçus par le CAH pour la période 2012-2013, pour un total de 178 dossiers depuis 2009. Le nombre de demandes va croissant, de même que le nombre de projets relatifs à la e-santé, dont la nature innovante bouscule le cadre posé par le Code de la santé publique. Au-delà de l'éclairage apporté par le CAH sur la procédure d'agrément elle-même **(1)**, le rapport du CAH contient également des préconisations concernant la mise en œuvre des projets nécessitant un agrément hébergeur **(2)**. Par ailleurs, tirant le bilan de cinq ans d'activité, le CAH propose des pistes de réforme et de modernisation du régime, dont tient compte le récent projet de loi sur la santé[5] **(3)**.

1. OBTENIR ET MAINTENIR UN AGREMENT HEBERGEUR DE DONNEES DE SANTE

Dans un secteur en pleine expansion, le rapport du CAH, en complément de la doctrine de l'ASIP Santé, permet de fournir des lignes directrices précieuses sur l'obtention d'un agrément, tant en ce qui concerne la demande initiale (**1.1**) que la demande de renouvellement (**1.2**).

1.1 Un périmètre à géométrie variable

Identifier les frontières du champ d'application de l'agrément a toujours été au cœur des débats sur ce régime. L'article L1111-8 du Code de la santé publique prévoit en effet un champ d'application *a priori* délimité, couvrant les cas où des données de santé recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins sont déposées chez un tiers par des professionnels de santé, des établissements de santé ou bien la personne concernée par les données. Néanmoins, tant l'ASIP Santé que le CAH démontrent une volonté continue d'interprétation large de ce champ d'application.

1.1.1 La position de l'ASIP Santé

Les premières questions sur ce point ont émané de secteurs d'activité (recherche, assurance…) aux frontières du champ d'application expressément prévu par le Code de la santé publique.

Sur la question de savoir si la procédure d'agrément couvre les recherches biomédicales, l'ASIP Santé parait répondre par l'affirmative[6], et ce, malgré l'opinion initialement exprimée par le CAH[7]. La position de l'ASIP Santé apparait similaire pour le secteur des assurances. Aucune recommandation formelle n'est venue confirmer cette interprétation pourtant lourde de conséquences. En tout état de cause, les termes de « *prévention, diagnostic ou soins* » ne doivent ainsi pas être entendus de manière restrictive.

---

[5] Projet de loi relatif à la santé, n° 2302, déposé le 15 octobre 2014.

[6] « *Le champ d'application de la procédure d'agrément s'applique à toute base de données recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins : recherche, secteur assurantiel.* » ASIP Santé, présentation du 10 février 2011 : « Le décret hébergeur : modalités d'application et questions d'actualité », Jeanne Bossi, secrétaire générale <http://esante.gouv.fr/sites/default/files/110208_JNI_JBO_Decret_Hebergeur_1.pdf>.

[7] Premier rapport d'activité du CAH pour les années 2006 à 2011.

De même, malgré la lettre de l'article L1111-8 qui ne fait référence qu'à des professionnels ou établissements de santé, le CAH précise que l'esprit de l'agrément est de couvrir les personnes tenues de collecter des données de santé du fait de leurs missions, même s'il ne s'agit pas de professionnels de santé, par exemple les établissements médico-sociaux, les centres de santé, les laboratoires de biologie médicale, ainsi que les prestataires de services de santé à domicile (PSAD).

L'évocation des PSAD par le CAH est d'autant plus intéressante que l'ASIP Santé a été amenée à examiner précisément la question de la soumission à agrément de l'hébergement des données de santé collectées par un PSAD ou par un distributeur de dispositif médical. Bien que les PSAD ne soient pas des professionnels de santé au sens du Code de la santé publique, ceux-ci sont réglementairement tenus de constituer un dossier de suivi des patients auprès desquels ils effectuent leurs prestations[8]. Dès lors, leur activité implique-t-elle d'obtenir un agrément hébergeur?

Certaines des données recueillies par le PSAD sont fournies par le patient ou le médecin, dans le cadre d'une activité de soin ; à ce titre, la lettre de l'article L1111-8 permettrait de considérer que les PSAD sont en principe compris dans le champ d'application de l'agrément. D'un autre côté, la majorité des données de suivi des patients sont collectées via les dispositifs médicaux ou les salariés du PSAD intervenant auprès du patient, ce qui n'est pas expressément prévu dans les textes.

Afin de permettre aux PSAD, de retrouver une certaine sécurité juridique, l'ASIP Santé a publié des lignes directrices à ce sujet[9]. Selon celles-ci, le PSAD qui héberge « *dans son propre système* » et « *localement* » des données de santé collectées dans le cadre de ses obligations réglementaires, peut dans certaines conditions ne pas être soumis à agrément. Le PSAD est en quelque sorte assimilé à un professionnel de santé, et « *comme pour l'établissement hospitalier (ou la clinique) hébergeant lui-même les données de santé des patients qu'il soigne, il y a ici unicité entre le producteur des données et celui qui les « héberge » lequel ne sera alors pas soumis au régime des hébergeurs »*[10].

Toutefois, selon l'ASIP Santé, l'absence d'obligation d'obtenir un agrément ne dispense pas le PSAD de respecter certaines dispositions du Code de la santé publique[11].

En outre, l'ASIP Santé précise que le PSAD doit être considéré comme responsable du traitement des données collectées dans le cadre de ses obligations réglementaires, au sens de la loi Informatique et Libertés[12]. La doctrine de l'ASIP Santé a donc comme corollaire que le PSAD ne pourrait pas se considérer comme un sous-traitant au sens de la loi Informatique et Libertés, position fréquemment défendue par les hébergeurs de données de santé. Dans ce cas,

---

[8] Arrêté du 19 décembre 2006, imposant au PSAD de constituer « *pour chaque personne prise en charge, un dossier contenant tous les éléments permettant le suivi de la personne, du matériel et service délivrés* ».

[9] « *Note juridique relative à l'hébergement de données de santé à caractère personnel aux dossiers détenus par les PSAD et les distributeurs de DM* », ASIP Santé, 21 mars 2012, <http://esante.gouv.fr/services/reperes-juridiques/note-juridique-relative-a-l-hebergement-de-donnees-de-sante-a-caractere#end>.

[10] « *Agrément des hébergeurs de données de santé : retour d'expérience* », Benoit LOUVET, Journal du Net, 19 mars 2013 <http://www.journaldunet.com/ebusiness/expert/53717/agrement-des-hebergeurs-de-donnees-de-sante---retour-d-experience.shtml>

[11] Il s'agit ici d'une application de l'alinéa 4 de l'article L1111-8 du Code de la santé publique aux PSAD et aux distributeurs de DMx, assimilés aux professionnels de santé et devant respecter l'article L1110-4 et les référentiels d'interopérabilité et de sécurité publiés par l'ASIP Santé.

[12] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004

le PSAD serait pleinement responsable devant la CNIL du respect des obligations prévues par la loi Informatique et Libertés.

1.1.2 La confirmation apportée par le CAH

L'ASIP Santé s'est ainsi constamment attachée à adapter le périmètre de l'agrément aux multiples métiers qui participent du parcours de soin.

Le rapport du CAH aborde par exemple la problématique des prestations d'hébergement dit « sec » ou en « salle blanche » où l'hébergeur ne fournit que l'infrastructure du data center où sont déposés les serveurs. Le professionnel de santé détient la propriété des serveurs et en assure lui-même l'exploitation. Le CAH estime que ce type d'hébergeur doit bien obtenir un agrément, malgré l'avis de représentants du secteur qui considèrent quant à eux que ce type de prestations ne correspond pas au rôle central d'un hébergeur agréé[13].

Il s'agit néanmoins d'un agrément limité, étant donné que toutes les garanties requises par le décret hébergeur en termes de sécurité logique ne seront pas exigées de l'hébergeur, qui assure surtout la sécurité physique des équipements. Le contrat entre l'établissement de santé et l'hébergeur devra refléter la réalité des rôles de chacun, en reportant sur l'établissement de santé presque toutes les obligations prévues par le décret et notamment celles relatives à la sécurité logique. De plus, l'hébergeur ne peut proposer ce type de prestations qu'à des professionnels de santé ou structures de soins, et non à des industriels ou éditeurs, afin d'éviter que cette dérogation ne soit utilisée pour contourner les obligations habituellement imposées à l'hébergeur.

Les applications et outils de « *quantified self* », ou de « mesure de soi » sont également analysés par le CAH. Ces applications permettent de « *mesurer et de comparer avec d'autres personnes des variables relatives à son mode de vie* »[14]. A ce titre, des données s'apparentant à des données de santé sont susceptibles d'être collectées par ces applications.

Compte tenu de l'utilisation croissante de ces applications par les particuliers, la nécessité d'obtenir un agrément hébergeur est une question essentielle, dont les répercussions sont tant juridiques qu'économiques. La CNIL ne s'est pas encore prononcée de façon définitive sur ce point et seules des hypothèses prospectives ont été envisagées[15]. Le CAH semble en revanche avoir voulu trancher le débat dans son rapport.

Qualifiant les données recueillies dans le cadre de la mesure de soi de « données de bien-être », le CAH estime que « *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* [...]. *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* ».

---

13 Communiqué de l'Association Française des Hébergeurs Agréés de Données de Santé à Caractère Personnel, « *Hébergement agréé - Quand la lettre tue l'esprit* », 12 novembre 2014, </ http://www.afhads.fr/?p=989 />

14 Communiqué de la CNIL, « *Quantified self, m-santé : le corps est-il un nouvel objet connecté ?* », 28 mai 2014, <www.cnil.fr/linstitution/actualite/article/article/quantified-self-m-sante-le-corps-est-il-un-nouvel-objet-connecte>

15 « *Le corps, nouvel objet connecté* » Cahiers IP - Innovation & Prospective n°02

Cette position a de quoi surprendre. L'implication d'un professionnel de santé n'est pas un critère posé par la loi et n'a pas d'influence sur la qualification juridique des données qu'une personne peut être conduite à remettre à un tiers. L'émergence de services liés à la santé directement accessibles aux patients, sans intervention d'un professionnel de santé, apparait plutôt constituer un risque qu'un critère de non-sensibilité des données. De plus, le fait que les données ne soient destinées qu'à améliorer les habitudes quotidiennes de l'individu n'exclut pas tout lien avec une pathologie. Le CAH propose comme illustration l'exemple d'un glucomètre, « *uniquement utilisé par la personne afin de contrôler sa glycémie et adapter ses habitudes alimentaires, sans qu'un professionnel de santé y ait accès* »[16]. Or, les mesures de la glycémie apparaissent tout particulièrement constituer un traitement de données relatives à une pathologie, dès lors qu'elles révèlent potentiellement le diabète, dont le suivi effectué de façon autonome par la personne s'apparente à une activité de prévention. Si certaines applications ne collectent en effet que des données non sensibles, d'autres révèlent des pathologies, potentielles ou avérées, qui peuvent atteindre le même degré de sensibilité que celles contenues dans un dossier médical.

En conséquence, il semblerait prudent de ne pas exclure trop rapidement ces activités du champ de l'agrément. Une approche au cas par cas pourrait être envisagée, selon la sensibilité des données collectées. Le décompte du nombre de pas par jour, ne nécessite pas le même niveau de protection que le suivi de la tension par une application. Une telle approche présente cependant une grande complexité et ne permet pas d'éviter les risques liés par exemple à un détournement de finalité ou un croisement des données faisant apparaitre des informations sensibles : l'innocuité d'une donnée peut difficilement être déterminée d'avance et avec certitude. A ce titre, des réponses appropriées devront être recherchées dans la pseudonymisation voire l'anonymisation des données à caractère personnel, la minimisation des données collectées, ainsi que dans la mise en œuvre du *privacy by design*.

1.2 Retour d'expérience des premières demandes de renouvellement

Le rapport du CAH fournit un aperçu intéressant de la démarche à adopter pour effectuer une demande de renouvellement, étant donné que jusqu'à présent, seule l'ASIP Santé avait communiqué sur les modalités du renouvellement, tout en se faisant l'écho des recommandations du CAH[17].

1.2.1 Le rappel à la rigueur par le CAH

Il ressort en effet du rapport du CAH que de façon générale, les dossiers manquent de rigueur et ne répondent pas aux exigences de la procédure d'agrément. Les chiffres publiés par le rapport révèlent par exemple que sur 96 dossiers reçus sur la période 2012-2013, 70 dossiers d'agréments seulement ont fait l'objet d'une analyse, pour moins d'une quarantaine d'agréés.

Ceci explique les raisons pour lesquelles l'ASIP Santé et le CAH se sont investis dans une démarche d'accompagnement des hébergeurs. Le rapport du CAH souligne à présent que l'activité d'hébergeur de données de santé nécessite de fournir un haut niveau de sécurité et de qualité: les renouvellements devront s'opérer sur la base de garanties solides.

---

[16] Rapport du CAH, préc. p.33

[17] ASIP Santé, Communiqué du 17 septembre 2013 <http://esante.gouv.fr/actus/politique-publique/hebergeurs-de-donnees-de-sante-le-point-sur-le-renouvellement-de-l-agrement>

1.2.2 Les éléments essentiels d'une demande de renouvellement

Ce qui parait essentiel de prime abord est la prise en compte des recommandations émises par le ministre en charge de la santé lors de l'agrément initial. Durant les premières années de la procédure d'agrément, le CAH a fait preuve d'une certaine souplesse en acceptant des dossiers qui n'étaient pas *stricto sensu* conformes, mais dont les carences ne constituaient pas « *des éléments de nature à entrainer un refus d'agrément* »[18] . L'agrément délivré précisait néanmoins les recommandations du ministre pour que l'hébergeur puisse améliorer sa prestation et remplir pleinement les critères requis. La bonne application des recommandations du ministre, du CAH et de la CNIL, accompagnant l'agrément initial constituera de ce fait un critère déterminant dans le renouvellement, afin de lever toutes les réserves. Le renouvellement d'agrément n'est pas une procédure qui peut être effectuée par un simple courrier : les hébergeurs doivent se préparer à une nouvelle analyse des garanties et justifier d'une amélioration continue de leur niveau de service[19].

Le CAH explicite également la portée de l'obligation d'indiquer les modifications apportées au service d'hébergement. L'hébergeur peut faire évoluer ses services, pour adapter ceux-ci aux demandes de ses clients, aux évolutions du cadre légal et doctrinal de son secteur, ainsi que celles de l'état de l'art technique. L'hébergeur dispose donc d'une certaine marge de manœuvre pour transformer son service sans avoir à effectuer une nouvelle demande d'agrément. Cette possibilité doit toutefois rester limitée aux évolutions non-substantielles, par exemple la modification des statuts, le recours à un nouveau sous-traitant, l'ajout d'un site d'hébergement, ou encore une nouvelle disposition de sécurité[20] . Ces évolutions ainsi que leur impact sur les documents initialement fournis à l'ASIP Santé doivent être clairement indiquées dans la demande de renouvellement. Le renouvellement ne peut pas en principe permettre à l'hébergeur d'élargir le périmètre de son agrément : dans un tel cas, l'hébergeur devra déposer un dossier de demande d'un nouvel agrément.

Effectuer une demande de renouvellement, c'est également fournir les résultats d'un audit réalisé par un auditeur tiers[21]. Là encore, l'ASIP Santé a publié un scenario d'audit de conformité et sécurité[22]. Dans son rapport, le CAH souligne néanmoins les difficultés de l'exercice, au vu des rapports reçus : périmètre de l'audit trop restreint, absence de propositions de remèdes, de documents essentiels... Plus inquiétant encore est le fait que certains audits ne formulent aucun constat de non-conformité concernant des dossiers dont l'analyse initiale par le CAH pointait les nombreux problèmes. Le risque d'audits de complaisance est à ce titre pointé par le CAH. Par conséquent, l'auditeur devra s'attacher à contrôler la conformité de l'intégralité des obligations imposées à l'hébergeur, en s'inspirant notamment de la matrice de couverture des exigences du décret hébergeur, publiée par l'ASIP Santé[23].

---

[18] Rapport du CAH, préc. p.7

[19] La procédure reprend ainsi une exigence fondamentale des processus qualité tels que la norme ISO : 9001

[20] ASIP Santé, Communiqué du17 septembre 2013 <http://esante.gouv.fr/actus/politique-publique/hebergeurs-de-donnees-de-sante-le-point-sur-le-renouvellement-de-l-agrement>

[21] Article R.1111-15 du Code de la Santé Publique

[22] Exemple d'audit de conformité et de sécurité, ASIP Santé, 14 mai 2014 <http://esante.gouv.fr/sites/default/files/HDS-Exemple-Audit_de_conformite-Securite_et_Technique_v1_0.pdf>

[23] Matrice de couverture des exigences du décret n°2006-6, publiée par l'ASIP Santé le 23 février 2010 <http://esante.gouv.fr/sites/default/files/Matrice_couverture_articles_decret2006_6v1.2.1.pdf>

2. LES QUESTIONS LIEES A LA MISE EN ŒUVRE DE L'HEBERGEMENT

Le rapport du CAH fait état des problématiques majeures rencontrées dans le cadre de la mise en œuvre de l'hébergement, qui concernent principalement la maitrise juridique (**2.1**) et technique des accès aux données de santé (**2.2**) ainsi que l'encadrement contractuel entre l'hébergeur et ses clients (**2.3**).

En revanche, il faut noter que le CAH ne relève pas de carence spécifique liée au chiffrement des données. Il s'agit pourtant d'une mesure de sécurité fondamentale, dont l'absence a conduit à l'unique sanction à ce jour publiquement imposée par la CNIL à un hébergeur agréé [24]. Le retour d'expérience du CAH sur ce point aurait été instructif.

2.1 Difficultés liées à la localisation des données de santé et habilitations d'accès

L'utilisation croissante du *cloud computing* est soulignée par le CAH comme problématique au regard des exigences du décret hébergeur. En effet, l'hébergement en *cloud* ne permet pas de déterminer à un instant *t* où se trouvent les données, tandis que le décret hébergeur suppose une « *localisation maitrisée* », et que « *la fonction d'hébergement tend à échapper à tout contrôle du fait de l'impossibilité de localisation des données à protéger* »[25].

Cependant, l'hébergeur est tenu de fournir lors de sa demande d'agrément une cartographie de son réseau précisant les sites d'hébergement, l'intervention de tiers, etc. Par conséquent, la localisation potentielle des données est connue et maitrisée. L'identification certaine de la localisation des données à un instant précis n'apparait pas fournir plus de garanties, dès lors que le périmètre géographique potentiel est identifié et agréé. A ce titre, et en théorie, l'hébergement en *cloud computing* n'implique pas nécessairement plus de risques qu'un hébergement classique impliquant des transferts vers des serveurs identifiés situés à l'étranger. L'ASIP Santé ne considère notamment pas que l'hébergement en *cloud computing* doive être encadré de façon spécifique, et se contente de rappeler les obligations imposées par la loi Informatique et Libertés[26].

Les garanties essentielles doivent porter sur les habilitations et les contrôles d'accès. Il est fréquent que les données de santé hébergées par un hébergeur agréé soient protégées par le secret médical.

Or, les textes définissent peu les personnes habilitées à accéder aux données de santé et surtout celles couvertes par le secret médical. Selon l'alinéa 7 de l'article L1111-8, l'hébergeur agréé ne peut donner accès aux données qu'aux « *personnes que celles-ci concernent et les professionnels de santé ou établissements de santé qui les prennent en charge et qui sont désignés par les personnes concernées* ». Or, de nombreuses personnes interviennent dans le système de santé sans être des professionnels de santé. Dans le cadre de leur activité, elles recueillent et sont parfois tenus réglementairement de recueillir, des données de santé couvertes par le secret médical. Leur intervention n'étant pas prévue par le décret hébergeur, l'ASIP Santé et le CAH ont été contraints de développer une doctrine innovante pour combler le vide juridique et adapter les dispositions légales à la réalité du système de santé. Ainsi, le CAH souligne que même l'accès par le médecin de l'hébergeur n'est pas expressément prévu par les textes ; que dire par ailleurs de toutes les professions

---

[24] Communiqué de la CNIL du 9 janvier 2012, <http://www.cnil.fr/linstitution/actualite/article/accessible/non/article/la-cnil-sanctionne-une-declaration-mensongere-dun-hebergeur-de-donnees-de-sante>

[25] Rapport du CAH, préc. p.13

[26] FAQ ASIP Santé, <http://esante.gouv.fr/services/referentiels/securite/hebergement-faq#22>

paramédicales qui reçoivent pourtant des données de santé dans l'exercice de leur mission ? Le rapport du CAH invite le législateur à intervenir, ce qui semble devoir être fait dans le projet de loi sur la santé déposé le 15 octobre 2014[27].

2.2 Le contrôle technique des accès

La problématique de l'accès se présente également sous une forme technique. La Carte de Professionnel de Santé (« CPS ») était initialement l'unique moyen prévu par les textes pour accéder aux données de santé. En raison du haut niveau de sécurité impliqué par la CPS et des difficultés pratiques rencontrées dans son déploiement, la possibilité d'utiliser un « *dispositif équivalent* » a été introduite[28].

Aucun exemple concret de dispositif équivalent n'avait été officiellement proposé par l'ASIP Santé jusqu'à la fin de l'année 2013 ; quelques mois avant, l'ASIP Santé avait même formellement rappelé qu'aucun dispositif équivalent n'avait encore été agréé et que l'utilisation d'une CPS demeurait impérative[29]. Pourtant, le rapport du CAH fait état de dossiers reposant sur des dispositifs alternatifs à la CPS. Pour ces raisons, le travail conjoint de l'ASIP Santé, du CAH et de la CNIL sur les messageries sécurisées de santé[30] semble avoir permis d'identifier des dispositifs équivalents qui pourraient désormais être agréés. Le rapport du CAH propose des dispositifs expressément indiqués comme permettant une authentification forte[31]. Le CAH constate que le niveau de sécurité de ces dispositifs n'est clairement pas équivalent à celui assuré par la CPS. Ceux-ci ne peuvent donc pas être utilisés comme alternative systématique à la CPS mais seulement lorsque la mise en œuvre d'une CPS est impossible ou inadéquate, et lorsqu'ils sont adaptés au niveau de risque identifié. Sous réserve du respect de ces conditions, il semble que les hébergeurs et leurs clients pourront désormais proposer plus aisément lors de leurs demandes d'agrément des modalités d'accès et d'identification nouveaux.

2.3 Les préconisations du CAH en termes contractuels

Le modèle de contrat d'hébergement à fournir au moment de la demande d'agrément est considéré par le CAH comme la pièce maitresse du dossier, et ne doit pas être négligé au bénéfice de la description des mesures techniques. Le CAH fournit dans son rapport des précisions, d'autant plus utiles qu'aucun contrat type n'est fourni par l'ASIP Santé.

Tout d'abord, le modèle de contrat doit être adapté à la spécificité du service, définir précisément le périmètre de celui-ci et fournir les annexes correspondantes (notamment les niveaux de services).

De plus, le CAH rappelle que le contrat doit impérativement traiter un certain nombre de clauses imposées par l'article R1111-13, ainsi que prévoir expressément certaines prestations inhérentes aux obligations de l'hébergeur, par exemple, l'organisation de la disponibilité et de la continuité du service ou bien la sauvegarde des données sur un site distant. Le CAH précise que certains thèmes doivent être couverts, qui ne sont pas expressément prévus par la loi :

---

[27] Projet de loi relatif à la santé, préc.

[28] Loi n° 2009-879 du 21 juillet 2009, article 132 modifiant l'article L1110-4 du Code de la santé publique. L'article R1110-3 du Code de la santé publique n'a cependant pas été mis à jour.

[29] Communiqué de l'ASIP Santé, 6 juin 2013, <http://esante.gouv.fr/actus/interoperabilite/cps-et-dispositifs-equivalents-le-point-de-l-asip-sante>

[30] Voir notamment délibération n° 2013-096 du 25 avril 2013 autorisant la mise en œuvre à titre expérimental du service national de « Messagerie Sécurisée de Santé » par l'Agence des Systèmes d'Information Partagés de Santé.

[31] Par exemple, utilisation d'un certificat logiciel de personne physique, ou d'un couple identifiant/mot de passe associé à un code d'accès unique.

politique d'habilitation, fonctions des personnels de maintenance, modalités de cession du contrat prévoyant l'obligation de cession à un hébergeur agréé. Le contenu du contrat n'est ainsi pas laissé à l'appréciation des parties.

En revanche, le CAH confirme la doctrine de l'ASIP Santé selon laquelle l'hébergeur peut choisir de reporter sur son client (ou sur ses sous-traitants) certaines des obligations dont il est en principe redevable aux termes du décret hébergeur. Cette liberté dans le partage des responsabilités est compréhensible dans la mesure où elle reflète une répartition opérationnelle des rôles. Néanmoins, les clients des hébergeurs n'étant généralement pas des professionnels de l'hébergement, il existe un risque que les hébergeurs se déchargent sur leurs clients d'obligations qui leur sont imposées par les textes, sans que cela ne réponde à une réalité opérationnelle. A tout le moins, quel que soit le choix des parties, l'hébergeur demeure redevable d'un devoir de conseil auprès de son client.

La liberté contractuelle des parties doit être défendue, mais eu égard aux constatations du CAH, il est permis de s'interroger sur la capacité des clients à obtenir un équilibre contractuel adéquat. Le CAH relève plusieurs exemples de clauses « faibles »: certains contrats ne mentionnent pas même de niveaux de services, d'autres n'identifient pas clairement les personnes habilitées à accéder aux données ou les moyens mis en œuvre pour exécuter le service... Le CAH fait également état de contrats prévoyant de larges exclusions de responsabilité : par exemple, exclusion de la responsabilité de l'hébergeur en cas d'intrusion frauduleuse, sans distinguer entre les intrusions par des tiers et les intrusions par le personnel de l'hébergeur. Pour le CAH, seules les premières pourraient faire l'objet d'une exclusion et l'hébergeur doit par conséquent prévoir cette distinction dans ses clauses. Incidemment, il peut paraitre également discutable pour un hébergeur agréé d'exclure totalement sa responsabilité en cas d'intrusion frauduleuse par un tiers, dès lors que le cœur de sa prestation concerne la sécurité des données.

3. DE NOUVELLES PERSPECTIVES

Le rapport du CAH annonce de nombreux changements, qui semblent d'ores et déjà se concrétiser dans le projet de loi sur la santé[32], et qui visent tant le périmètre de l'agrément (**3.1**), que l'obligation du recueil du consentement de la personne (**3.2**) ainsi que la nature même de l'agrément délivré (**3.3**).

3.1 La consécration d'une interprétation large du périmètre de l'agrément

La doctrine du CAH et de l'ASIP Santé se trouve confirmée, notamment en ce qui concerne le périmètre de l'hébergement. Le projet de loi prévoit en effet de réécrire l'article L.1111-8, pour supprimer la condition liée à la qualité des personnes à l'origine du dépôt des données.

Le premier alinéa se trouve entièrement refondu en disposant que « *toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic ou de soins pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil desdites données ou pour le compte du patient lui-même, doit être agréée à cet effet* ». Il n'y a plus de distinction entre les personnes effectuant les dépôts des données, le critère principal demeurant l'activité ayant donné lieu à la production ou au recueil des données. On ne peut que saluer cette simplification.

---

32 Projet de loi relatif à la santé, préc.

De même, l'obligation de conserver les données de santé sur des systèmes d'informations conformes aux référentiels d'interopérabilité et de sécurité élaborés par l'ASIP Santé est élargie : aux termes du projet de loi, cette obligation serait étendue à « *tout autre organisme participant à la prévention, aux soins, ou au suivi médico-social et social* »[33]. . Faut-il comprendre ainsi que ces organismes participant aux activités de prévention, de soin et de suivi seraient, pour ces activités, assimilés aux professionnels de santé ? A ce titre, l'hébergement de données de santé sur leurs systèmes d'information ne serait pas considéré comme une externalisation entrainant l'obligation d'obtenir un agrément hébergeur ou d'utiliser les services d'un hébergeur agréé ? Ceci rejoindrait en tout cas la position actuelle de l'ASIP Santé, par exemple en ce qui concerne les PSAD et les distributeurs de dispositifs médicaux.

3.2 La suppression du recueil du consentement des personnes

L'un des changements essentiels apporté par le projet de loi est la remise en cause du consentement des personnes comme fondement à la licéité de l'hébergement[34]. Le CAH constatait déjà dans son rapport que l'obligation de recueillir le consentement exprès des patients à l'hébergement de ses données de santé est délicate à mettre en oeuvre, notamment pour les nouveaux services ne se résumant plus au seul hébergement de dossiers patients informatisés[35].

Par ailleurs, les exceptions au recueil du consentement semblent aujourd'hui dépasser la règle, que ce soit lorsque le consentement n'a pas à être recueilli quand les données hébergées ne sont accessibles qu'au patient et au professionnel de santé seuls[36], ou lorsqu'il est réputé avoir déjà été accordé pour les données actuellement hébergées par les établissements publics ou privés de santé[37]. A titre d'illustration, le CAH rappelle également que dans le cadre des messageries sécurisées de santé (MSS), la CNIL a reconnu qu'il n'était « *pas réaliste d'exiger un recueil du consentement à chaque échange ou pour chaque nouveau destinataire* »[38]. L'autorisation unique adoptée par la suite ne fait pas même état du consentement[39]. Il faut relever cependant que dans sa délibération, la CNIL s'était également appuyée sur les dispositions de l'article L.1110-4, qui subordonne les échanges entre plusieurs professionnels de santé d'informations relatives à une personne prise en charge à l'absence d'opposition de la personne dûment avertie, et non à son consentement. La CNIL avait également signalé que« *le recueil d'un consentement initial, matérialisé par la remise d'un document papier ou électronique et assorti d'une faculté de révocation à tout moment, aurait été de nature à permettre l'exercice des droits des personnes sans paralyser la mise en œuvre ultérieure de la MSS* ». La suppression de l'obligation de consentement ne va pas de soi.

---

33 Le projet de loi dans sa rédaction actuelle prévoit la suppression de l'alinéa 4 de l'article L.1111-8 et la création d'un nouvel article L.1110-4-1 dans le Code de la santé publique.

34 Refonte du premier alinéa de l'article L. 1111-8 du Code de la santé publique et suppression de la dernière phrase du deuxième alinéa ainsi que de l'intégralité de la cinquième phrase.

35 Rapport du CAH, préc. p.20

36 Article L1111-8 al. 5 du Code de la santé publique

37 Article 29 de la loi n° 2011-940 du 10 août 2011

38 Délibération n° 2013-096 du 25 avril 2013 autorisant la mise en œuvre à titre expérimental du service national de « Messagerie Sécurisée de Santé » par l'ASIP Santé (Demande d'autorisation n° 1639657).

39 Autorisation unique n° AU-037 - Délibération n° 2014-239 du 12 juin 2014 portant autorisation unique de mise en œuvre, de traitements de données à caractère personnel ayant pour finalité l'échange par voie électronique de données de santé à travers un système de messagerie sécurisée

Il est en effet possible de s'interroger sur la difficulté réelle pour les hébergeurs ou les professionnels de santé à recueillir le consentement. Par ailleurs, compte tenu du niveau d'information à fournir, il semble qu'une forme de consentement sera de toute façon demandée au patient, aux fins de preuve de la bonne exécution de ses obligations d'information par l'hébergeur ou par le professionnel de santé. La difficulté réside surtout dans le fait d'obtenir un consentement libre, en permettant donc aux personnes d'exercer leur droit d'opposition. Le CAH souligne en effet qu'il « *apparait illusoire de pouvoir respecter en pratique le droit d'opposition du patient à l'égard de l'hébergement externalisé de ses données* » : aujourd'hui, beaucoup de systèmes ne permettent pas, en pratique, de cesser le traitement automatisé d'un dossier au cas par cas. La CNIL avait également relevé cette problématique[40]. Or, le fait de cesser de demander le recueil du consentement exprès ne signifie pas que les personnes ne seront plus en mesure d'exercer leur droit d'opposition. A cet égard, le CAH recommande, comme alternative au consentement, de « *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* ». La suppression de l'obligation de consentement exprès risque ainsi de ne pas résoudre pleinement la problématique liée à la liberté de choix du patient.

3.3 Le passage d'un agrément à une certification

Enfin, le projet de loi prévoit la possibilité de remplacer l'agrément par *« une accréditation par l'instance nationale d'accréditation »*. Il s'agirait ainsi de transférer au COFRAC la responsabilité de la procédure d'agrément, qui deviendrait une démarche de certification. Le CAH évoquait déjà cette possibilité dans son rapport, en proposant de s'orienter vers une procédure similaire à celle existant dans le domaine bancaire (*Payment Card Industry Data Security Standard*). Ceci permettrait de supprimer l'instruction imposée tant à la CNIL qu'au CAH, « *redondante sur la quasi-totalité des points d'analyse* » selon le CAH ; au-delà de l'allègement en termes de coûts, ce transfert de compétences permettrait aux pouvoirs publics de se concentrer sur les contrôles, aujourd'hui rares dans ce domaine. Le CAH souhaiterait même qu'une procédure spécifique de contrôle des hébergeurs soit créée, en complément de ceux déjà effectués par la CNIL. Quelle que soit l'évolution de la procédure, les hébergeurs agréés ou certifiés devraient ainsi se préparer à un accroissement des contrôles.

L'objectif avoué de cette évolution est de permettre au régime de l'agrément de sortir de sa spécificité nationale et ainsi d'être transposé au niveau communautaire[41]. Le régime actuel présente en effet l'avantage d'inciter les opérateurs à un haut niveau de sécurité de leurs systèmes d'information, tout en leur permettant d'être reconnus sur le marché . Le secteur de la santé étant un des plus touché par les failles de sécurité[42], un renforcement des standards au niveau communautaire paraitrait tout à fait pertinent.

Toutefois, le régime français d'agrément des hébergeurs représente une contrainte presque sans équivalent dans les autres ordres juridiques, et ce, même dans l'Union européenne. Depuis que ce régime est en vigueur, il n'a pas réussi à convaincre de façon à être transposé

---

40 « Les règles de fonctionnement de la MSS ne doivent pas paralyser son utilisation, ni dissuader les professionnels de santé de l'utiliser, ce qui pourrait être le cas s'il fallait vérifier à chaque échange que le consentement n'a pas été révoqué. »

41 Exposé des motifs du projet de loi relatif à la santé publique, art.51.

42 Voir notamment les statistiques de l'autorité de protection des données personnelles au Royaume-Unis (Information Commissionner's Office) qui publie régulièrement des statistiques concernant les failles de sécurité notifiées, et qui révèlent notamment que le secteur de la santé est de loin celui qui effectue le plus de notifications (160 à 195 notifications par trimestre pour les quatre derniers trimestres pour le secteur de la santé, tandis que les secteurs Internet ou Télécom ne génèrent qu'un maximum respectif de cinq notifications par trimestre)<http://ico.org.uk/enforcement/trends>).

dans d'autres juridictions, malgré la forte croissance du secteur de la e-santé. Il faut également compter avec les dispositions du projet de règlement européen sur la protection des données à caractère personnel[43], qui ne vont pas non plus dans le sens d'un renforcement spécifique de la protection des données de santé. Le nouveau régime de certification envisagé par le projet de loi sur la santé devra ainsi relever le défi de la transposition dans d'autres ordres juridiques, voire au niveau de l'Union européenne, sans quoi il est à craindre que le droit français ne puisse plus imposer seul ce régime unique en son genre.

43 Proposition de règlement publiée par la Commission le 25 janvier 2012 < http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf > . Voir aussi le texte de compromis adopté par la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) le 21 octobre 2013, Rapport du Parlement européen du 22 novembre 2013, , COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).