Loi de modernisation de notre système de santé
Une lecture critique par l'AFHADS

Montceau les Mines, le 22 janvier 2016

La loi adoptée le 17 décembre 2015 au terme d'un long processus représente pour les hébergeurs de données de santé (HDS) une avancée significative, devant leur permettre d'assumer mieux, avec plus de réactivité et de lisibilité leurs missions de protection des données personnelles qui leur sont confiées et de support des pratiques coopératives de soins.

Toutefois, ce texte dense et éclectique ne pouvait aller dans un niveau de détail suffisant pour comprendre le cadre exact dans lequel s'exercera leur activité. Nombre de décisions cruciales sont reportées à des arrêtés, ordonnances ou référentiels encore à paraître.

Avec ce document, l'AFHADS souhaite contribuer à la finalisation du travail engagé sur trois volets essentiels pour ses membres :

- La portée de l'agrément
- La restriction des destinataires des données hébergées
- Le référentiel de certification des HDS

La portée de l'agrément

Le texte originel de l'article fondateur de l'agrément, l'article L1111-8 du Code de la Santé Publique, autorisait les établissements et professionnels de santé, ou la personne concernée, à déposer les données de santé à caractère personnel (DSCP) auprès d'hébergeurs agréés.

Dans sa nouvelle version, c'est l'hébergeur qui est soumis à la contrainte de l'agrément s'il reçoit des DSCP recueillies à l'occasion d'activités de prévention, de diagnostic, de soins, de suivi social ou médico-social. On retombe alors sur le problème classique de la responsabilité de l'hébergeur sur les contenus. Les hébergeurs généralistes français peuvent prendre la précaution d'interdire de tels contenus dans leurs conditions générales de vente. En cas de faute, ils pourront alors se retourner contre leur client indélicat.

En revanche, cette nouvelle rédaction semble permettre un contournement consistant à faire héberger les données dans un pays tiers. Dans ce cas aucun recours direct ou indirect ne semble possible envers l'opérateur ou l'établissement qui en serait à l'initiative.

La protection par le L1111-8 n'existant plus, un verrou subsiste pour les producteurs de DSCP soumis à un régime d'autorisation préalable par la CNIL. La pratique constante sur ces demandes d'autorisation est un rappel de l'obligation de recourir à un hébergeur agréé. Par contre, les

professionnels et établissements de soins n'ont besoin que d'une déclaration normale ou d'une inscription au registre de leur Correspondant Informatique et Libertés. L'ordonnance à venir devra rétablir l'obligation explicite de recours à un hébergeur agréé afin d'éviter cette dérive.

Il y a également une ambiguïté à lever sur la mise en place des Groupements Hospitaliers de Territoire (GHT). L'établissement support est chargé de mettre en place un dossier patient, potentiellement partagé dans les conditions de respect des règles d'interopérabilité et de sécurité qui s'appliquent également aux HDS.

Cette précision quant aux règles de partage semble mettre l'établissement en dehors du périmètre de l'agrément. Pourtant, il s'agit bien d'une personne morale hébergeant des DSCP pour le compte d'autres personnes morales à l'origine de la production desdites données. Aucune interprétation n'ouvre donc la porte à une dispense d'agrément.

Au-delà de l'interprétation des textes, c'est aussi une question de bon sens et d'équité. La qualité d'établissement de santé ne confère aucune protection particulière par rapport aux menaces informatiques, et les mêmes exigences sont applicables à tous.

La dérogation accordée aux établissements dès lors que l'accès aux données était réservé à leur propre usage et à la personne concernée ne serait pas applicable dans ce cas de figure. En effet, un directeur d'établissement peut faire le choix d'assumer ses propres risques informatiques, mais pas de les propager en dehors de sa structure.

Enfin, l'argument d'impuissance compte tenu des ressources limitées attribuées à la délivrance des agréments ne tient plus avec la transformation de l'agrément en certification. La logique voudrait même qu'à terme, après quelques années de rodage, le référentiel de certification des HDS soit intégré au référentiel de certification HAS des établissements afin de garantir aux patients une sécurité optimale de leurs données quelle que soit la méthode de déploiement du système d'information.

Les destinataires des données hébergées

Dans la version originelle du L1111-8, il était indiqué que seules peuvent accéder aux données les personnes concernées et les professionnels ou établissements de santé qui les prennent en charge.

Cette formulation devait être adaptée avec l'extension aux domaines médico-social et social. Elle a donc été remplacée par « Les personnes physiques ou morales à l'origine de la production de soins ou du recueil des données ». On a malencontreusement perdu au passage les personnes concernées.

Une restriction similaire se retrouve dans deux autres paragraphes. L'un concerne les destinataires des données, passant de 'les professionnels et établissements de santé désignés dans le contrat d'hébergement' à 'les personnes qui les ont confiées'.

L'autre concerne la restitution des données en fin d'hébergement, passant de 'la personne ayant contracté avec l'hébergeur' à 'les personnes qui les lui ont confiées'.

Outre l'exclusion malvenue de la personne concernée, on voit également mal comment, dans un dossier collaboratif, par exemple de coordination des soins, l'hébergeur pourrait restituer à chacun des professionnels prenant en charge le patient les données qu'il aurait déposées.

Un travail d'interprétation est ici nécessaire pour neutraliser des dispositions qui sont de toute façon superfétatoires par rapport à la déclaration des destinataires dans les procédures CNIL.

Le référentiel de certification

Au terme du processus législatif, la certification des hébergeurs intègre bien, comme le souhaitait l'AFHADS, leur capacité à qualifier les applications hébergées. C'est cette dimension qui justifie la spécificité du métier des HDS et leur valeur ajoutée.

Le but de la certification doit être de démontrer que l'hébergeur candidat possède et mobilise la capacité de concevoir des environnements d'exécution à un niveau de sécurité approprié par rapport aux risques propres à chaque application. En effet, l'un des travers du processus actuel était que le dossier d'agrément figeait les solutions mises en œuvre, alors que la diversité et l'évolutivité des applications exige une adaptation à chaque cas particulier.

A cet effet, on pourra utilement s'appuyer sur un référentiel reconnu internationalement tel que la série ISO 27000, ce qui aidera également les HDS à défendre leur offre au-delà des frontières nationales.

Sur la spécificité additionnelle qu'est la qualification des applications, elle doit clairement se faire envers les nouveaux référentiels de sécurité et d'interopérabilité prévus pour l'ensemble des acteurs de la prévention, des soins, du suivi médico-social et social. On parvient ainsi à un niveau homogène d'exigence sur la sécurité des données pour toutes les situations d'hébergement d'une application, que ce soit au sein d'un établissement ou chez un hébergeur agréé tiers (établissement support d'un GHT, groupement de coopération sanitaire ou acteur privé). L'obligation de qualification des applications par les hébergeurs permet même d'entrainer dans cette démarche vertueuse les nombreux acteurs, par exemple du secteur assurantiel ou du « quantified self », qui sans y être obligés font le choix de recourir à un HDS pour en tirer un avantage concurrentiel.

La certification des hébergeurs n'est alors plus un signe de défiance envers des acteurs extérieurs au système sanitaire, mais bien la continuité logique d'une vraie démarche de sécurité au service des patients et la garantie de son application aux nouveaux services de prise en charge coopérative et au secteur médico-social.