

J.O n° 113 du 16 mai 2007

Commission nationale de l'informatique et des libertés

Délibération n°2006-293 du 21 décembre 2006 portant avis sur un projet de décret en Conseil d'Etat relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique

NOR: CNIX0710374X

La commission, saisie le 20 novembre 2006 par le ministre de la santé et des solidarités d'un projet de décret en Conseil d'Etat pris en application des dispositions de l'article L. 1110-4 du code de la santé publique relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique,

Vu la Convention n°108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

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

Vu la 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 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu le code de la santé publique, et notamment son article L. 1110-4 ;

Vu le code de la sécurité sociale, et notamment ses articles L. 161-36-1 A et L. 161-36-2 ;

Vu la délibération de la CNIL n°2005-209 du 11 octobre 2005 portant avis sur un projet de décret en Conseil d'Etat relatif à la confidentialité des données de santé à caractère personnel pris en application de l'article L. 1110-4 du code de la santé publique ;

Après avoir entendu M. Jean-Pierre de Longevialle, commissaire, en son rapport et Mme Pascale Compagnie, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

Le ministre de la santé et des solidarités a saisi la Commission nationale de l'informatique et des libertés d'une nouvelle version du projet de décret en Conseil d'Etat relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique. Ce texte pris en application des dispositions du quatrième alinéa de l'article L. 1110-4 du code de la santé publique (issu de l'article 3 de la loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé) qui dispose :

« Afin de garantir la confidentialité des informations médicales mentionnées aux alinéas précédents, leur conservation sur support informatique comme leur transmission par voie électronique entre professionnels sont soumises à des règles définies par décret en Conseil d'Etat pris après avis public et motivé de la Commission nationale de l'informatique et des libertés. Ce décret détermine les cas où l'utilisation de la carte professionnelle de santé mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale est obligatoire. »

Cette disposition a été insérée à l'article L. 161-36-1 A du code de la sécurité sociale par la loi du 13 août 2004 relative à l'assurance maladie, qui prévoit notamment la création du dossier médical personnel (DMP) et précise que le report dans ce dossier par les professionnels de santé des informations médicales qu'ils génèrent s'opère dans le respect des règles de sécurité prévues à l'article L. 1110-4 du code de la santé publique.

Sur le renvoi à des référentiels définis par arrêté

Alors que le premier projet de décret pris en application de l'article L. 1110-4 du code de la santé publique, dont la commission a été saisie et sur lequel elle s'est prononcée par avis du 11 octobre 2005, renvoyait la définition précise des règles de sécurité applicables à la conservation et à la transmission sur support électronique des données personnelles de santé à des « politiques de confidentialité » consignées dans des « protocoles de

confidentialité » établis par les professionnels et établissements de santé, le présent texte dispose que les conditions de confidentialité et de sécurité auxquelles auront à se conformer les professionnels et établissements de santé seront précisées dans des « référentiels » définis par arrêté du ministre de la santé pris après avis de la CNIL et conformes, pour les établissements publics de santé et ceux participant à un service public hospitalier, au référentiel général de sécurité instauré par l'ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

La commission approuve pleinement l'évolution que traduit le nouveau dispositif qui ne fait plus reposer la responsabilité d'établir les règles de sécurité sur ceux auxquels il incombe de les appliquer.

Elle se félicite également que, conformément à la demande formulée dans son précédent avis, le texte dont elle est aujourd'hui saisie comporte aux 1°, 2°, 3° et 4° du projet d'article R. 1110-1 du code de la santé publique l'énumération qu'elle avait souhaitée des catégories de mesures à adopter pour parvenir à un contenu satisfaisant des règles de sécurité.

Si la commission comprend par ailleurs que soit recherchée une cohérence entre les référentiels relatifs aux conditions de confidentialité et de sécurité applicables aux informations médicales et le référentiel général de sécurité instauré par l'ordonnance du 8 décembre 2005, elle estime que, s'agissant de données de santé qui sont protégées par un secret légal, les règles de sécurité doivent être renforcées par rapport à celles applicables dans le domaine de l'administration électronique.

De toute façon, elle observe que le référentiel général de sécurité prévu à l'article 9 de l'ordonnance du 8 décembre 2005 « fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique... » alors que l'objet des référentiels applicables aux données de santé devra être plus large et couvrir non seulement la transmission de ces données mais également leur conservation sur support électronique.

Enfin, il y a lieu de rappeler que les établissements privés de soins ne sont pas hors du champ d'application des règles de sécurité. Or, en ce qui les concerne, le projet de décret ne contient aucune indication.

Mais le problème qui a particulièrement retenu l'attention de la commission est celui que pose la date d'entrée en vigueur de ces dispositions. En effet, aux termes de l'article 2 du projet de décret, cette date devrait intervenir dans un délai maximum de trois ans à compter de la publication de l'arrêté du ministre de la santé, qui définira le référentiel de sécurité applicable aux données de santé. Comme, ainsi qu'il vient d'être précisé, ce dernier référentiel devra lui-même être (pour partie) conforme au référentiel général de sécurité de l'ordonnance du 8 décembre 2005 et que celle-ci a prévu que « les conditions d'élaboration, d'approbation, de modification et de publication de ce référentiel sont fixées par décret », à ce jour non paru, on voit que la mise en oeuvre effective des règles de sécurité à fixer en application d'une disposition législative remontant à 2002 se trouve en réalité reportée à une date qui risque d'être très lointaine.

Pour que ces délais d'application soient compatibles avec le calendrier de mise en place du DMP et l'objectif annoncé de « généralisation » de celui-ci au 1er juillet 2007, la Commission estime en conséquence nécessaire que soient prévues des dispositions transitoires relatives aux règles de sécurité qui devront s'appliquer pendant la période qui s'écoulera entre la publication du décret et l'entrée en vigueur des référentiels approuvés par le ministre de la santé.

Sur l'utilisation de la carte de professionnel de santé

Concernant l'utilisation de la carte de professionnel de santé, qui ne constituera qu'un élément des référentiels de sécurité applicables aux données de santé, mais un élément particulièrement important, l'article L. 1110-4 déjà mentionné dispose que le décret pris pour son application « détermine les cas dans lesquels cette utilisation est obligatoire ».

Le projet d'article R. 1110-3 du code de la santé publique a pour effet de rendre obligatoire cette utilisation ou celle d'un dispositif d'identification individuel offrant des garanties et fonctionnalités similaires et agréé par le ministre de la santé dans tous les cas d'accès à un fichier automatisé contenant des données personnelles de santé ou de transmission de données de santé par voie électronique.

En particulier, aucune distinction n'est faite par ce texte pour la transmission électronique de données de santé selon que cette transmission a lieu entre professionnels ou établissements de santé et à l'intérieur d'un établissement de santé au sein ou en dehors de la structure d'exercice.

La commission ne peut qu'être favorable à un emploi aussi généralisé que possible de la CPS qui permet à son porteur d'attester de son identité et de sa qualité de professionnel, de se faire reconnaître d'une application afin

d'accéder à des informations médicales dans le respect des droits liés à sa fonction, de signer électroniquement et de procéder à un chiffrement des messages pour garantir la confidentialité de l'échange.

Cependant, la commission constate que la CPS est encore peu utilisée dans les établissements de santé. Aussi bien, si les dispositions de l'article R. 1110-3 seraient applicables immédiatement aux professionnels de santé, elles n'entreraient en vigueur, pour les établissements de santé, que « dans un délai qui ne peut être supérieur à trois ans à compter de la publication » du décret.

Dès lors, sur ce point également, la commission ne peut que réitérer les questions soulevées précédemment et le constat qui a été fait de la nécessité de prévoir un dispositif qui s'appliquerait jusqu'à la mise en place des règles définitives.

Enfin, dans la mesure où la CNIL est une autorité administrative indépendante qui a notamment pour mission de s'assurer du respect de la sécurité des données à caractère personnel, il apparaît utile que l'agrément du ministre soit délivré après avis de la CNIL.

Le président,

A. Türk