

J.O n° 113 du 16 mai 2007

Commission nationale de l'informatique et des libertés

Délibération 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

NOR: CNIX0710381X

Saisie le 26 janvier 2005 par le ministre des solidarités, de la santé et de la famille, 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 données de santé à caractère personnel,

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, modifiée par la loi du 6 août 2004, relative à l'informatique, aux fichiers et aux libertés ;

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 ;

Après avoir entendu M. Jean-Pierre de Longevialle, commissaire, en son rapport et Mme Catherine Pozzo di Borgo, commissaire adjoint du Gouvernement, en ses observations,

Emet l'avis suivant :

Le ministre des solidarités, de la santé et de la famille, a saisi la Commission nationale de l'informatique et des libertés du projet de décret en Conseil d'Etat relatif à la confidentialité des données de santé à caractère personnel pris en application des dispositions du quatrième alinéa de l'article L. 1110-4 du code de la santé publique.

Ces dispositions sont ainsi rédigées : « 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. »

Ces dispositions ont été insérées à l'article L. 161-36-1 (A) du code de la sécurité sociale par l'article 2-I de la loi du 13 août 2004 portant réforme de l'assurance maladie, article qui précède immédiatement celui portant création du dossier médical personnel (DMP) rendant ainsi le respect et la mise en oeuvre de ces dispositions nécessaires pour la mise en place du DMP. L'article L. 1110-4 du code de la santé publique est également directement visé à l'article L. 161-36-2 du code de la sécurité sociale qui traite des conditions d'utilisation du dossier médical personnel.

Sur l'obligation de définir une politique de confidentialité

L'article R. 1110-1 du projet de décret impose à tout professionnel de santé exerçant à titre libéral ou tout établissement, réseau de santé ou organisme participant à la prévention et aux soins, qui conserve sur support informatique ou transmet par voie électronique des informations médicales à caractère personnel portées à sa connaissance, en particulier pour assurer la continuité des soins ou déterminer la meilleure prise en charge sanitaire possible, de définir une politique de confidentialité décrivant les règles et l'organisation nécessaires pour garantir la protection de ces informations, ainsi que la sécurité des traitements dont elles ont fait l'objet.

Cette politique de confidentialité devra préciser, en particulier, les règles d'accès aux informations ainsi que les

conditions dans lesquelles elles sont échangées entre professionnels de santé. Elles seront définies de façon différente selon qu'elles sont échangées entre les membres de l'équipe de soins en charge de cette personne ou, sous réserve de la non-opposition de la personne dûment avertie, avec d'autres professionnels exerçant dans la structure de prise en charge ou à des professionnels extérieurs à cette structure.

Aux termes de l'article R. 1110-4 du projet de décret, le responsable des traitements au sens de l'article 3 de la loi du 6 janvier 1978 modifiée est chargé de mettre en oeuvre la politique de confidentialité du système d'information. Il gère la liste nominative des professionnels de santé habilités à accéder aux données médicales visées à l'article R. 1110-1 et met en oeuvre les procédés permettant de garantir l'authentification des professionnels de santé habilités. En particulier, il est garant de la cohérence entre les données d'identification gérées localement et celles figurant dans l'annuaire du groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale.

A cet égard, l'article R. 1110-6 du projet de décret prévoit d'ores et déjà l'obligation, pour le responsable du traitement, de mettre à disposition de toute personne concernée une notice résumant les principales dispositions de la politique de confidentialité, et notamment les règles d'accès aux données médicales, les traitements autorisés et leur finalité. Une liste actualisée de tous les professionnels de santé ayant accès aux données de santé à caractère personnel ainsi que ceux auxquels elles ont été transmises devra également être établie.

La commission prend acte de ces dispositions qui n'appellent pas d'observation particulière.

La politique de confidentialité devra être précisée dans un protocole de confidentialité soumis au contrôle de la commission dans le cadre des formalités préalables prévues par la loi du 6 janvier 1978.

Toutefois, afin de respecter la volonté du législateur qui, à l'article L. 1110-4 du code de la santé publique, a précisément renvoyé au décret le soin de définir les règles nécessaires pour garantir la confidentialité des informations médicales, leur conservation sur support informatique comme leur transmission par voie électronique entre professionnels, la commission estime que le projet de décret devrait comporter une énumération des mesures de sécurité qui devront figurer dans le protocole de confidentialité.

A cet effet, la commission propose que les dispositions de l'alinéa premier de l'article R. 1110-2 du projet de décret soient rédigées de la façon suivante :

« Un protocole de confidentialité définit les moyens assurant la mise en oeuvre des dispositions prévues à l'article R. 1110-1 et, en particulier :

« a) Les mesures de sécurisation physiques des matériels et des locaux ainsi que, le cas échéant, les dispositions à prendre pour les sauvegardes des fichiers ;

« b) Les modalités d'accès physiques et logiques aux traitements, en particulier les mesures d'identification et d'authentification des utilisateurs et le recours éventuel à un dispositif d'accès par carte à puce ou un dispositif analogue ;

« c) Les dispositifs de contrôle des habilitations et les procédures de traçabilité des accès aux données, et en particulier le système de journalisation des connexions mis en place ;

« d) Les mesures mises en place pour assurer la confidentialité des données par le recours à un dispositif de codage des données nominatives ou de chiffrement de tout ou partie des données notamment en cas de transmission de données de santé à caractère personnel par réseau (internet, wifi...) ; l'indication du recours à la CPS ou à un dispositif de certification logicielle équivalent. »

Sur le recours à la carte de professionnel de santé

L'article R. 1110-3 du projet de décret impose désormais aux professionnels de santé qui accèdent aux données de santé à caractère personnel de s'identifier et de s'authentifier. Le second alinéa de l'article précise : « L'utilisation de la carte de professionnel de santé mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale ou, par dérogation, d'un certificat logiciel équivalent inscrit sur un support de nature à en garantir la fiabilité et l'unicité, gérée par l'autorité de certification visée à l'article R. 161-54 du code de la sécurité sociale et décrit dans le protocole de confidentialité précité est obligatoire pour l'authentification des professionnels de santé qui transmettent des données à caractère personnel en dehors de leur structure d'exercice. »

La commission prend acte que le projet de décret consacre l'utilisation de la carte de professionnel de santé, carte à puce délivrée à tout professionnel de santé identifié comme tel auprès du Groupement d'intérêt public de la carte de professionnel de santé (GIP-CPS) visé à l'article R. 161-54 du code de la sécurité sociale, comme outil

d'identification et d'authentification dès lors que des données de santé à caractère personnel sont transmises en dehors de la structure d'exercice.

La carte de professionnel de santé permet à son porteur d'attester de son identité et de sa qualité de professionnel, de se faire connaître d'une application afin d'accéder à des informations dans le respect des droits liés à sa fonction, de signer électroniquement les opérations qu'il effectue afin de les valider et de garantir la non-altération des données et de procéder à un chiffrement des messages pour garantir la confidentialité de l'échange.

La CNIL rappelle qu'elle a, de façon constante, tout particulièrement depuis le développement des dispositifs en réseau, rappelé dans ses avis, que le recours à la CPS était prioritaire par rapport à un dispositif de login/password, beaucoup moins efficace pour garantir la sécurisation des échanges. L'obligation ainsi posée de recourir à la CPS pour la transmission de données personnelles de santé est donc de nature à satisfaire la commission dans la mesure où son utilisation renforce le niveau de sécurité des dispositifs informatiques qui comportent des données sensibles.

Toutefois, dans la mesure où la carte de professionnel de santé n'est pas diffusée dans tous les lieux de soins, le projet de décret prévoit que l'utilisation de la CPS peut être remplacée par un certificat logiciel équivalent également géré par l'autorité de certification qu'est le GIP-CPS. La commission propose, à l'article R. 1110-3 du projet de décret, de préciser les termes utilisés en adoptant la rédaction suivante : « dispositif d'authentification individuel offrant des garanties similaires et agréé par le groupement d'intérêt public mentionné à l'article R. 161-54 ».

Enfin, la commission estime que les dispositions de l'article R. 1110-7 relatif aux hébergeurs de données de santé à caractère personnel n'entrent pas dans le champ d'application du décret. Le projet d'article devrait donc être disjoint.

L'article 2 du projet de décret prévoit que les professionnels de santé, établissements, réseaux ou structures mentionnés à l'article R. 1110-1 du code de la santé publique qui, à la date de publication du présent décret, assurent les opérations mentionnées au même article doivent, dans le délai de deux ans à compter de cette publication, transmettre à la Commission nationale de l'informatique et des libertés un document attestant qu'ils se sont mis en conformité avec les dispositions dudit décret. La commission propose, dans un souci de simplification des formalités incombant aux professionnels de santé qui, pour la plupart, ont déjà déclaré leur application, de maintenir le délai de deux ans, mais de supprimer la mention de la transmission à la CNIL de tout document, celle-ci se réservant le droit de procéder à tout contrôle sur pièces et sur place.

Le président,

A. Türk