Décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique

Le Président de la République,

Sur le rapport du Premier ministre et du ministre de la santé et des solidarités,

Vu le code du patrimoine, notamment le titre Ier du livre II ;

Vu le code de la santé publique, notamment ses articles L. 1111-7, L. 1111-8 et L. 1112-1 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, notamment ses articles 21 et 24 ;

Vu le décret n° 79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques ;

Vu le décret n° 97-34 du 15 janvier 1997 modifié relatif à la déconcentration des décisions administratives individuelles, notamment son article 2 ;

Vu le décret n° 97-1185 du 19 décembre 1997 modifié pris pour l'application à la ministre de l'emploi et de la solidarité du 1° de l'article 2 du décret du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;

Vu l'avis du Conseil national de l'ordre des médecins en date du 1er avril 2004 ;

Vu l'avis du Conseil national de l'ordre des chirurgiens-dentistes en date du 8 avril 2004 ;

Vu l'avis du Conseil national de l'ordre des pharmaciens en date du 11 mai 2004 ;

Vu l'avis du Conseil national de l'ordre des sages-femmes en date du 26 mai 2004 ;

Vu les avis de la Commission nationale de l'informatique et des libertés en date des 27 mai 2004 et 15 mars 2005 ;

Le Conseil d'Etat (section sociale) entendu ;

Le conseil des ministres entendu,

Décrète :

Article 1

Le chapitre Ier du titre Ier du livre Ier de la première partie du code de la santé publique (dispositions réglementaires) est ainsi modifié :

I. - La section unique devient la sous-section 1, intitulée « Sous-section 1 : Accès aux informations de santé à caractère personnel », au sein d'une section 1 dont le titre est ainsi rédigé :

« Section 1

« Principes généraux »

II. - Après l'article R. 1111-8, il est ajouté une sous-section 2 ainsi rédigée :

« Sous-section 2

« Hébergement des données de santé à caractère personnel

« Art. R. 1111-9. - Toute personne physique ou morale souhaitant assurer l'hébergement de données de santé à caractère personnel, mentionné à l'article L. 1111-8, et bénéficier d'un agrément à ce titre doit remplir les conditions suivantes :

« 1° Offrir toutes les garanties pour l'exercice de cette activité, notamment par le recours à des personnels qualifiés en matière de sécurité et d'archivage des données et par la mise en oeuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la

conservation et la restitution des données confiées, ainsi qu'un usage conforme à la loi ;

« 2° Définir et mettre en oeuvre une politique de confidentialité et de sécurité, destinée notamment à assurer le respect des exigences de confidentialité et de secret prévues par les articles L. 1110-4 et L. 1111-7, la protection contre les accès non autorisés ainsi que la pérennité des données, et dont la description doit être jointe au dossier d'agrément dans les conditions fixées par l'article R. 1111-14 ;

« 3° Le cas échéant, identifier son représentant sur le territoire national au sens de l'article 5 de la loi du 6 janvier 1978 ;

« 4° Individualiser dans son organisation l'activité d'hébergement et les moyens qui lui sont dédiés, ainsi que la gestion des stocks et des flux de données ;

« 5° Définir et mettre en place des dispositifs d'information sur l'activité d'hébergement à destination des personnes à l'origine du dépôt, notamment en cas de modification substantielle des conditions de réalisation de cette activité ;

« 6° Identifier les personnes en charge de l'activité d'hébergement, dont un médecin, en précisant le lien contractuel qui les lie à l'hébergeur.

« Art. R.* 1111-10. - L'agrément nécessaire à l'activité d'hébergement de données de santé à caractère personnel est délivré par le ministre chargé de la santé, qui se prononce après avis de la Commission nationale de l'informatique et des libertés et d'un comité d'agrément placé auprès de lui.

« A cet effet, la personne intéressée adresse au ministre chargé de la santé un dossier de demande d'agrément comprenant les éléments mentionnés à l'article R. 1111-12. Le ministre transmet le dossier à la Commission nationale de l'informatique et des libertés, qui apprécie les garanties présentées par le candidat à l'agrément en matière de protection des personnes à l'égard des traitements de données de santé à caractère personnel et de sécurité de ces données. La commission rend son avis dans un délai de deux mois à compter de la réception du dossier, délai pouvant être renouvelé une fois sur décision motivée de son président.

« Dès que la commission s'est prononcée ou à l'expiration du délai qui lui était imparti, elle transmet la demande d'agrément, accompagnée, le cas échéant, de son avis, au comité d'agrément mentionné au premier alinéa. Ce comité se prononce sur tous les aspects du dossier, en particulier sur les garanties d'ordre éthique, déontologique, technique, financier et économique qu'offre le candidat. Il émet son avis dans le mois qui suit la réception du dossier transmis par la Commission nationale de l'informatique et des libertés. Il peut toutefois demander un délai supplémentaire d'un mois.

« Le ministre chargé de la santé dispose, pour prendre sa décision, d'un délai de deux mois suivant l'avis du comité d'agrément. A l'issue de ce délai, son silence vaut décision de rejet.

« Art. R. 1111-11. - I. - Le comité d'agrément mentionné à l'article R. 1111-10 comprend :

« 1° Un membre de l'inspection générale des affaires sociales nommé sur proposition du chef de l'inspection générale des affaires sociales ;

« 2° Deux représentants des associations compétentes en matière de santé, agréées au niveau national dans les conditions prévues à l'article L. 1114-1 ;

« 3° Deux représentants des professions de santé, l'un nommé sur proposition du Conseil national de l'ordre des médecins et l'autre sur proposition de l'Union nationale des professions de santé ;

« 4° Trois personnalités qualifiées :

« a) Une personne choisie en raison de ses compétences dans les domaines de l'éthique et du droit ;

« b) Une personne choisie en raison de ses compétences en matière de sécurité des systèmes d'information et de nouvelles technologies ;

« c) Une personne choisie en raison de ses compétences dans le domaine économique et financier.

« Le directeur général de la santé, le directeur de l'hospitalisation et de l'organisation des soins, le directeur des Archives de France, le directeur général des entreprises et le directeur général de la concurrence, de la consommation et de la répression des fraudes, ou leurs représentants, assistent aux séances du comité avec voix consultative.

« II. - Les membres du comité d'agrément, dont celui qui, parmi eux, exercera la présidence du comité, sont nommés pour cinq ans par arrêté du ministre chargé de la santé. Leur mandat est renouvelable une fois.

« Lors de leur entrée en fonction, les membres du comité adressent au président une déclaration mentionnant toute activité personnelle ou professionnelle en rapport direct ou indirect avec les missions du comité, ainsi que les liens directs ou indirects qu'ils peuvent avoir avec tout organisme hébergeant ou

susceptible d'héberger des données de santé à caractère personnel ou avec les organismes professionnels et les sociétés de conseil intervenant dans le domaine de compétence du comité. Ils s'engagent à signaler toute modification concernant cette situation.

« Ils ne peuvent siéger lorsque est examinée une affaire relative à un organisme au sein duquel ils détiennent un intérêt, exercent des fonctions ou détiennent un mandat, ou au sein duquel ils ont, au cours des dix-huit mois précédant la séance, détenu un intérêt, exercé des fonctions ou détenu un mandat.

« Des suppléants en nombre égal au nombre de titulaires sont désignés dans les mêmes conditions que ceux-ci. Un membre titulaire empêché ou intéressé par une affaire est remplacé par son suppléant.

« Le remplacement d'un membre du comité en cas de cessation de fonction en cours de mandat est réalisé dans les mêmes conditions que sa nomination et pour la durée du mandat restant à courir.

« Les fonctions de membre du comité ouvrent droit à des indemnités pour frais de déplacement et de séjour dans les conditions prévues par les dispositions législatives et réglementaires applicables aux fonctionnaires civils de l'Etat.

« III. - Le comité d'agrément ne peut délibérer que si deux tiers au moins de ses membres sont présents. Dans le cas contraire, une nouvelle séance peut se tenir sans obligation de quorum après un délai de quinze jours.

« Les avis rendus par le comité sont motivés. Ils sont pris à la majorité des voix exprimées des membres présents. En cas de partage égal des voix, celle du président est prépondérante.

« IV. - Le comité d'agrément peut être saisi par le ministre chargé de la santé de tout sujet entrant dans son domaine de compétence.

« Art. R. 1111-12. - Le dossier de demande d'agrément comprend les éléments suivants :

« 1° L'identité et l'adresse du responsable du service d'hébergement et, le cas échéant, de son représentant ; pour les personnes morales, les statuts sont produits ;

« 2° Les noms, fonctions et qualifications des opérateurs chargés de mettre en oeuvre le service, ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont accès aux données hébergées ;

« 3° L'indication des lieux dans lesquels sera réalisé l'hébergement ;

« 4° Une description du service proposé ;

« 5° Les modèles de contrats devant être conclus, en application du deuxième alinéa de l'article L. 1111-8, entre l'hébergeur de données de santé et les personnes physiques ou morales qui sont à l'origine du dépôt des données de santé à caractère personnel ; ces modèles sont établis conformément aux dispositions de l'article R. 1111-13 ;

« 6° Les dispositions prises pour assurer la sécurité des données et la garantie des secrets protégés par la loi, notamment la présentation de la politique de confidentialité et de sécurité prévue au 2° de l'article R. 1111-9 ;

« 7° Le cas échéant, l'indication du recours à des prestataires techniques externes et les contrats conclus avec eux ;

« 8° Un document présentant les comptes prévisionnels de l'activité d'hébergement et, éventuellement, les trois derniers bilans et la composition de l'actionnariat du demandeur, ainsi que, dans le cas d'une demande de renouvellement, les comptes de résultat et bilans liés à cette activité d'hébergement depuis le dernier agrément.

« L'hébergeur déjà agréé informe sans délai le ministre chargé de la santé de tout changement affectant les informations mentionnées ci-dessus et de toute interruption, temporaire ou définitive, de son activité.

« Art. R. 1111-13. - Les modèles de contrats devant être joints à la demande d'agrément, mentionnés au 5° de l'article R. 1111-12, contiennent obligatoirement au moins les clauses suivantes :

« 1° La description des prestations réalisées : contenu des services et résultats attendus ;

« 2° Lorsque le contrat est souscrit par la personne concernée par les données hébergées, la description des modalités selon lesquelles les professionnels de santé et les établissements de santé les prenant en charge et désignés par eux peuvent être autorisés à accéder à ces données ou en demander la transmission et l'indication des conditions de mise à disposition de ces données ;

« 3° Lorsque le contrat est souscrit par un professionnel de santé ou un établissement de santé, la description des modalités selon lesquelles les données hébergées sont mises à leur disposition, ainsi que les conditions de recueil de l'accord des personnes concernées par ces données s'agissant tant de leur hébergement que de leurs modalités d'accès et

de transmission ;

« 4° La description des moyens mis en oeuvre par l'hébergeur pour la fourniture des services ;

« 5° La mention des indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, ainsi que de la périodicité de leur mesure ;

« 6° Les obligations de l'hébergeur à l'égard de la personne à l'origine du dépôt des données de santé à caractère personnel en cas de modifications ou d'évolutions techniques introduites par lui ;

« 7° Une information sur les conditions de recours à d'éventuels prestataires techniques externes et les engagements de l'hébergeur pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement ;

« 8° Une information sur les garanties permettant de couvrir toute défaillance éventuelle de l'hébergeur ;

« 9° Une présentation des prestations à la fin de l'hébergement.

« Art. R. 1111-14. - Une présentation de la politique de confidentialité et de sécurité, prévue au 2° de l'article R. 1111-9, doit être fournie à l'appui de la demande d'agrément conformément au 6° de l'article R. 1111-12. Elle comporte notamment les précisions suivantes :

« 1° En matière de respect des droits des personnes concernées par les données hébergées :

« a) Les modalités permettant de s'assurer de l'existence du consentement de l'intéressé à l'hébergement des données le concernant ;

« b) Les modalités retenues pour que l'accès aux données de santé à caractère personnel et leur transmission éventuelle n'aient lieu qu'avec l'accord des personnes concernées et par les personnes désignées par elles ;

« c) Les conditions dans lesquelles sont présentées et prises en compte les éventuelles demandes de rectification des données de santé à caractère personnel hébergées ;

« d) Les moyens mis en oeuvre pour assurer le respect des dispositions de l'article L. 1111-7 relatif à l'accès des personnes à leurs informations de santé, notamment en termes de délais et de modalités de consultation ;

« e) Les procédures de signalement des incidents graves, dont l'altération des données ou la divulgation non autorisée des données personnelles de santé ;

« f) La fourniture à la personne concernée par les données hébergées, à sa demande, de l'historique des accès aux données et des consultations ainsi que du contenu des informations consultées et des traitements éventuellement opérés.

« 2° En matière de sécurité de l'accès aux informations :

« a) Les dispositions prises pour garantir la sécurité des accès et des transmissions des données de santé à caractère personnel vis-à-vis des établissements ou des professionnels de santé à l'origine du dépôt et des personnes concernées par ces données ;

« b) Les mesures prises en matière de contrôle des droits d'accès et de traçabilité des accès et des traitements ;

« c) Les conditions de vérification du contenu des traces des accès et des traitements afin de détecter les tentatives d'effraction ou d'accès non autorisés ;

« d) Les modalités de vérification du registre des personnes habilitées à accéder aux données hébergées tenant compte des éventuelles mises à jour ;

« e) Les procédés techniques retenus en matière d'identification et d'authentification ; en ce qui concerne les professionnels de santé, ces procédés techniques doivent avoir été agréés par le groupement d'intérêt public mentionné à l'article R. 161-54 du code de la sécurité sociale.

« 3° En matière de pérennité des données hébergées :

« a) Les procédures visant à assurer, au moment du transfert des données vers l'hébergeur, la réception sécurisée des données et l'intégrité de celles-ci, leur prise en compte dans le système d'information de l'hébergeur et le suivi de cette prise en charge ;

« b) Les modalités de prise en compte et d'enrichissement tout au long de la durée de l'hébergement, de l'ensemble des informations concernant les données depuis leur création, telles que les données permettant de les identifier et de les décrire, de les gérer, de déterminer leurs propriétés techniques et d'en assurer la traçabilité ;

« c) Les modalités de surveillance des supports en vue d'anticiper les changements technologiques et, le cas échéant, d'opérer des migrations de supports dans des conditions en garantissant la traçabilité ;

« d) Les procédures liées à la réplication des données sur différents supports informatiques en des lieux distincts ;

« e) Les conditions de mise en oeuvre d'une alerte concernant les formats d'encodage des données, destinée à avertir la personne à l'origine du dépôt en cas d'obsolescence de ce format et, éventuellement, les procédures visant à réaliser, avec l'autorisation de la personne à l'origine du dépôt, des migrations de formats des données, si ces derniers ne permettent plus d'assurer la lisibilité des informations et à assurer la traçabilité de ces migrations.

« 4° En matière d'organisation et de procédures de contrôle interne en vue d'assurer la sécurité des traitements et des données :

« a) La désignation d'un responsable sécurité et d'un responsable qualité ;

« b) La définition des missions, des pouvoirs et des obligations des personnels de l'hébergeur et de ses éventuels sous-traitants, habilités à traiter les données de santé à caractère personnel ;

« c) Les spécifications techniques des logiciels et des mécanismes de sécurité propres à garantir la confidentialité des transmissions, notamment en ce qui concerne le mode de chiffrement des flux d'information ;

« d) Les modalités retenues pour l'évaluation périodique des risques et l'audit des mesures de protection mises en place afin de garantir la sécurité des données et en vue d'apporter les modifications nécessaires en cas de détection de défaillances ;

« e) Les dispositifs de simulation régulière de défauts de fonctionnement pour vérifier l'efficacité des mécanismes destinés à garantir la continuité des services ;

« f) Les moyens mis en oeuvre pour sensibiliser et former le personnel aux mesures de protection mises en place et à leurs obligations en matière de confidentialité et de respect du secret professionnel ;

« g) Les conditions de mise en oeuvre de la sécurité physique des sites informatiques, des mesures de protection de l'infrastructure technique, notamment en termes de sécurité des réseaux, des serveurs et des postes de travail ;

« h) Les dispositions prises en ce qui concerne l'exploitation de l'infrastructure technique ;

« i) Les conditions de mise en oeuvre du plan de secours informatique comportant notamment les dispositions prises pour informer du déclenchement de ce plan les personnes physiques ou morales à l'origine du dépôt des données de santé à caractère personnel ainsi que les dispositions prises pour la reprise des activités.

« Art. R. 1111-15. - L'agrément est délivré aux hébergeurs de données de santé à caractère personnel pour une durée de trois ans.

« La demande de renouvellement doit être déposée au plus tard six mois avant le terme de la période d'agrément. Elle comprend les documents mentionnés au 8° de l'article R. 1111-12 et un récapitulatif des modifications intervenues depuis la dernière demande d'agrément en ce qui concerne les autres documents mentionnés à cet article, ainsi qu'un audit externe réalisé aux frais de l'hébergeur, attestant de la mise en oeuvre de la politique de confidentialité et de sécurité mentionnée à l'article R. 1111-14. Elle est instruite selon la même procédure que celle applicable à la demande initiale.

« Les décisions d'agrément, ainsi que le renouvellement de cet agrément, sont publiées au Bulletin officiel du ministère de la santé.

« Art. R. 1111-16. - Le ministre chargé de la santé, lorsqu'il envisage de procéder au retrait d'un agrément en application du quatrième alinéa de l'article L. 1111-8, communique à l'hébergeur intéressé, par lettre recommandée avec demande d'avis de réception, les motifs de ce projet de retrait et l'appelle à formuler ses observations, écrites ou, à sa demande, orales, dans un délai de deux mois.

« En cas de divulgation non autorisée de données de santé à caractère personnel ou de manquements graves de l'hébergeur à ses obligations mettant notamment en cause l'intégrité, la sécurité et la pérennité des données hébergées, le ministre chargé de la santé peut, à titre conservatoire, dans l'attente qu'il soit statué définitivement sur le projet de retrait d'agrément, prononcer la suspension de l'activité d'hébergement.

« La décision de retrait est notifiée à l'hébergeur intéressé, par lettre recommandée avec demande d'avis de réception. Elle met fin de plein droit à l'hébergement des données confiées à l'hébergeur et entraîne la restitution de ces données aux personnes ayant contracté avec l'hébergeur.

« Les décisions de suspension et de retrait font l'objet de la mesure de publicité prévue à l'article R. 1111-15. Elles sont transmises pour information au comité d'agrément mentionné à l'article R. 1111-10 ainsi qu'à la Commission nationale de l'informatique et des libertés. »

Article 2

I. - Après le premier alinéa de l'article R. 1111-2 du code de la santé publique, il est inséré un alinéa ainsi rédigé :

« Dans le cas où les informations demandées sont détenues par un établissement de santé et si les dispositifs techniques de l'établissement le permettent, le demandeur peut également consulter par voie électronique tout ou partie des informations en cause. »

II. - L'article R. 1112-7 du même code est remplacé par les dispositions suivantes :

« Art. R. 1112-7. - Les informations concernant la santé des patients sont soit conservées au sein des établissements de santé qui les ont constituées, soit déposées par ces établissements auprès d'un hébergeur agréé en application des dispositions à l'article L. 1111-8.

« Le directeur de l'établissement veille à ce que toutes dispositions soient prises pour assurer la garde et la confidentialité des informations ainsi conservées ou hébergées.

« Le dossier médical mentionné à l'article R. 1112-2 est conservé pendant une durée de vingt ans à compter de la date du dernier séjour de son titulaire dans l'établissement ou de la dernière consultation externe en son sein. Lorsqu'en application des dispositions qui précèdent, la durée de conservation d'un dossier s'achève avant le vingt-huitième anniversaire de son titulaire, la conservation du dossier est prorogée jusqu'à cette date. Dans tous les cas, si la personne titulaire du dossier décède moins de dix ans après son dernier passage dans l'établissement, le dossier est conservé pendant une durée de dix ans à compter de la date du décès. Ces délais sont suspendus par l'introduction de tout recours gracieux ou contentieux tendant à mettre en cause la responsabilité médicale de l'établissement de santé ou de professionnels de santé à raison de leurs interventions au sein de l'établissement.

« A l'issue du délai de conservation mentionné à l'alinéa précédent et après, le cas échéant, restitution à l'établissement de santé des données ayant fait l'objet d'un hébergement en application de l'article L. 1111-8, le dossier médical peut être éliminé. La décision d'élimination est prise par le directeur de l'établissement après avis du médecin responsable de l'information médicale. Dans les établissements publics de santé et les établissements de santé privés participant à l'exécution du service public hospitalier, cette élimination est en outre subordonnée au visa de l'administration des archives, qui détermine ceux de ces dossiers dont elle entend assurer la conservation indéfinie pour des raisons d'intérêt scientifique, statistique ou historique. »

III. - Le délai de conservation des dossiers médicaux fixé à l'article R. 1112-7 du code de la santé publique s'appliquera à l'issue d'un délai de douze mois suivant la publication du présent décret.

Article 3

Au 2 du titre II de l'annexe au décret n° 97-1185 du 19 décembre 1997, le tableau intitulé « code de la santé publique » est ainsi complété :

Vous pouvez consulter le tableau dans le JO

n° 4 du 05/01/2006 texte numéro 14

Article 4

Les dispositions du présent décret peuvent être modifiées par décret en Conseil d'Etat, à l'exception de celles qui déterminent la compétence du ministre chargé de la santé figurant à l'article R.* 1111-10 du code de la santé publique et de celles de l'article 3 du présent décret dont la modification ne peut intervenir que dans les conditions prévues à l'article 2 du décret du 15 janvier 1997.

Article 5

Le Premier ministre, le ministre de la santé et des solidarités et le ministre de la culture et de la communication sont responsables, chacun en ce qui le concerne, de l'application du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 4 janvier 2006.