Projet présenté par le Conseil d'Etat

Date de dépôt: 20 septembre 2005
Messagerie

Projet de loi
sur le réseau communautaire d'informatique médicale du système de santé du canton de Genève (e-toile) (K 3 07)

Le GRAND CONSEIL de la République et canton de Genève
décrète ce qui suit :

Chapitre I Dispositions générales

Art. 1 Objet et buts

La présente loi régit la mise en place d'un réseau communautaire d'informatique médicale destiné à améliorer la qualité des soins dans le respect strict de la protection des données personnelles des patients.

Art. 2 Définitions

Réseau

[1] On entend par réseau la connexion électronique des données de patients détenues par les prestataires de soins.

Clé d'accès

[2] On entend par clé d'accès l'élément matérialisé, par exemple une carte, donnant un accès individuel à tout ou partie des données du réseau concernant un patient.

Système d'identification personnelle

[3] On entend par système d'identification personnelle l'élément servant à sécuriser l'identification et l'authentification du détenteur de la clé d'accès par le biais d'un code.

ATAR ROTO PRESSE – 450 ex. – 10-2005

Patient

[4] On entend par patient la personne qui adhère au réseau et qui peut avoir recours à un prestataire de soins.

Médecin de confiance

[5] Le médecin de confiance est un médecin qui a adhéré au réseau et qui est choisi en cette qualité par le patient.

Prestataires de soins

[6] Les prestataires de soins sont les personnes fournissant des soins et bénéficiant d'une autorisation de pratiquer dans le canton de Genève, les établissements de soins, les pharmacies, les laboratoires d'analyses médicales et les instituts de radiologie au bénéfice d'une autorisation d'exploiter dans le canton de Genève. Les entités médicales spécialisées situées dans un autre canton avec lesquelles le canton de Genève a conclu un accord de collaboration sont également considérées comme des prestataires de soins au sens de la présente loi.

Fondation

[7] On entend par fondation la fondation IRIS, chargée de promouvoir, de gérer et de faire évoluer le réseau.

Département

[8] On entend par département le département de l'action sociale et de la santé du canton de Genève.

Episode de soins

[9] On entend par épisode de soins la période durant laquelle il existe une relation thérapeutique continue entre un prestataire de soins et un patient.

Art. 3 Champ d'application personnel

[1] Toute personne physique habitant ou exerçant une activité professionnelle dans le canton de Genève peut demander à adhérer au réseau.

[2] Tout prestataire de soins peut demander à adhérer au réseau et à obtenir une clé d'accès.

Art. 4 Personnes n'ayant pas le plein exercice des droits civils

[1] Les mineurs et interdits capables de discernement ont les mêmes droits et devoirs que les autres patients au sens de la présente loi. S'ils le désirent, ils peuvent être assistés par leur représentant légal.

[2] Si la personne est incapable de discernement, ses droits sont exercés par le représentant qu'elle avait préalablement désigné à cette fin ou par son représentant légal.

Art. 5 Liberté d'entrer et de sortir du réseau

[1] Les patients et les prestataires de soins sont libres d'adhérer ou non au réseau.

[2] Le patient rattaché au réseau depuis plus d'une année peut en sortir pour la fin d'une année civile.

[3] Le prestataire de soins rattaché au réseau depuis plus de trois ans peut en sortir pour la fin d'une année civile, moyennant un préavis de trois mois donné à la Fondation.

Art. 6 Prohibition de discriminer

Les patients et les prestataires de soins qui refusent d'adhérer au réseau ne peuvent faire l'objet d'aucune mesure discriminatoire.

Art. 7 Principes généraux de protection des données

Légalité et bonne foi

[1] Un traitement de données personnelles dans le cadre du réseau ne peut être entrepris que d'une manière licite.

[2] Tout traitement de données doit respecter le principe de la bonne foi.

Proportionnalité

[3] Les données concernant un patient ne peuvent être traitées que dans l'intérêt de ce dernier et dans la mesure où une activité thérapeutique le justifie.

[4] L'utilisation à des fins statistiques de données anonymisées ne permettant pas de remonter aux patients est permise.

Sécurité des données

[5] Les données des patients doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques correspondant au standard de qualité déterminé périodiquement par la Fondation.

Exactitude des données

[6] Quiconque enregistre ou modifie des données personnelles doit s'assurer qu'elles sont exactes.

Art. 8 Rectification ou effacement de données inexactes

[1] Le patient peut requérir la rectification ou l'effacement des données inexactes ou périmées le concernant dans les plus brefs délais et gratuitement.

[2] La rectification ou l'effacement de données fait que celles-ci ne sont plus accessibles. Seule la mention de la date de la modification est enregistrée dans le dossier.

[3] Toute modification est protocolée en précisant son auteur et la date de son intervention.

[4] Si un intérêt légitime le justifie, tout intéressé peut requérir le Tribunal de première instance ou la commission de surveillance compétente au sens de la loi sur la santé du … *(date d'adoption)* ou l'organe de surveillance de l'article 14 de la présente loi de consulter une donnée rectifiée ou effacée ou de la rendre accessible dans la mesure nécessaire. Si la requête intervient dans une procédure en cours, l'autorité saisie la transmet à l'autorité compétente.

Chapitre II Organisation du réseau

Art. 9 Caractéristiques du réseau

[1] Le réseau permet d'accéder par voie électronique aux dossiers de patients tenus par les différents prestataires de soins ayant adhéré au réseau.

[2] Sont prohibés la constitution d'un dossier centralisé de patient, agrégeant les dossiers de plusieurs prestataires de soins, et son exportation vers un autre système informatique.

Art. 10 Médecin de confiance

Rôle

[1] Le médecin de confiance est le conseiller du patient pour tout ce qui relève des données médicales le concernant.

[2] Il explique au patient les informations contenues dans son dossier et l'aide à définir les droits d'accès aux différentes catégories de données.

[3] Il signale au patient l'éventuelle interconnexion du réseau communautaire d'informatique médicale avec d'autres réseaux d'informations.

Libre choix

[4] Le patient choisit librement un ou plusieurs médecins de confiance, parmi les médecins ayant adhéré au réseau.

[5] Il peut modifier ou révoquer en tout temps ses choix.

Art. 11 Registre

[1] La Fondation tient un registre de tous les prestataires de soins rattachés au réseau.

[2] Ce registre est public et peut être consulté gratuitement.

[3] La Fondation tient un registre confidentiel de tous les patients ayant adhéré au réseau.

Art. 12 Dossier du patient

[1] Chaque prestataire de soins tient un dossier informatisé du patient conformément aux principes de sa profession et aux prescriptions légales en vigueur.

[2] Les dispositions légales concernant la conservation du dossier du patient sont applicables.

Art. 13 Equipement

[1] Les prestataires de soins demandant leur rattachement au réseau doivent disposer de l'équipement et des services standards déterminés par la Fondation.

[2] Le département accorde des subventions pour l'acquisition de ces équipements et services, selon les modalités définies par le Conseil d'Etat.

Art. 14 Surveillance du réseau

[1] Le réseau est soumis à la surveillance d'un organe indépendant désigné par le Conseil d'Etat.

[2] Cet organe veille à ce que le réseau respecte sa charte, les règles d'éthique médicale et de protection des données.

Art. 15 Clé d'accès

[1] Le patient qui adhère au réseau reçoit une clé d'accès personnelle.

[2] Les clés d'accès au réseau sont émises sous la responsabilité et le contrôle de la Fondation.

Chapitre III Accès aux données et transmission

Art. 16 Catégories de données

[1] Les données concernant le patient sont réparties dans les catégories ci-dessous.

Données administratives

[2] Les nom, prénom, adresse et date de naissance du patient, le nom de la caisse-maladie et d'autres assurances maladie ou accidents, l'étendue de la couverture d'assurance.

Données utilitaires

[3] A sa demande expresse et dans les limites définies par le patient, les directives anticipées, les décisions relatives au don d'organes, les personnes à aviser en cas d'urgence ainsi que les données médicales que tous les prestataires de soins ont un intérêt reconnu à pouvoir consulter sans retard, telles que des allergies, un traitement spécifique (par exemple anticoagulant) ou une affection spéciale, telle que le diabète.

Données médicales

[4] Toutes les pièces concernant le patient, notamment l'anamnèse, le résultat de l'examen clinique et des analyses effectuées, l'évaluation de la situation du patient, les soins proposés et ceux effectivement prodigués, avec l'indication de l'auteur et de la date de chaque inscription.

Données stigmatisantes

[5] Les données médicales dont la divulgation pourrait porter atteinte à la vie sociale ou privée du patient, selon sa propre appréciation ou après avoir pris conseil auprès du médecin de confiance.

Données secrètes

[6] Le patient peut demander au prestataire de soins, indépendant par rapport à une équipe de soins, de faire le nécessaire afin que ses données médicales ne soient pas accessibles sur le réseau.

Art. 17 Accès aux données

Principes

[1] Sous réserve des alinéas 9, 10 et 12 du présent article, l'accès aux données nécessite la clé d'accès du patient et celle d'un prestataire de soins ainsi que leurs codes d'identification.

[2] Le réseau doit permettre un accès sélectif en fonction de la catégorie de données et des droits d'accès attribués au prestataire de soins.

[3] L'accès aux données ou à certaines catégories d'entre elles doit être rendu impossible pour toute personne non habilitée.

[4] Le réseau doit être conçu de manière à empêcher la mise en relation de données nominales concernant plusieurs patients.

Par le patient

[5] Avec sa seule clé d'accès, le patient a le droit de consulter en tout temps les données qui le concernent ; ce droit ne s'étend pas aux notes rédigées par le professionnel de santé exclusivement pour son usage personnel, ni aux données concernant des tiers et protégées par le secret professionnel.

[6] Le patient a le droit se faire expliquer les données par un médecin de confiance qui doit le recevoir à cette fin dans un délai raisonnable.

[7] Le médecin de confiance commente les données du patient et s'enquiert de leur bonne compréhension.

Par le médecin de confiance

[8] Le médecin de confiance est habilité, en présence du patient et avec la clé d'accès de ce dernier, à accéder à toutes les données concernant le patient.

[9] Moyennant une autorisation spéciale du patient, révocable en tout temps, le médecin de confiance peut accéder à tout ou partie des données du patient, même en son absence.

Par les autres prestataires de soins

[10] Tout prestataire de soins qui traite une personne ayant adhéré au réseau a accès en tout temps, avec sa seule clé d'accès, aux données administratives et aux données utilitaires.

[11] Avec la clé d'accès du patient, il a accès aux données médicales strictement nécessaires à sa mission dans l'épisode de soins concerné.

En cas d'urgence

[12] Tout médecin rattaché au réseau, directement ou par le biais d'un établissement de soins, est habilité, avec sa seule clé d'accès, à consulter les données médicales d'un patient dont la vie ou la santé est menacée d'un danger imminent.

[13] Toute consultation de données médicales effectuée dans ces circonstances est signalée automatiquement au médecin de confiance du patient qui en contrôle le bien-fondé et tient à disposition du patient le journal d'accès à ses données.

Chapitre IV Sécurité de la transmission des données

Art. 18 Cryptage

[1] Toutes les données du réseau doivent être cryptées de manière à ce que leur accès soit strictement limité aux personnes habilitées. Le cryptage doit être effectué en fonction des types de données et doit correspondre au meilleur standard disponible en Suisse.

[2] Les règles de cryptage font l'objet d'un règlement élaboré par la Fondation.

Art. 19 Identification personnelle

Toute personne souhaitant accéder aux données doit s'identifier au moyen de la clé d'accès et du système d'identification personnelle.

Art. 20 Attestation de réception

Toute personne qui consulte des données doit en confirmer la réception par le biais de sa clé d'accès et du système d'identification personnelle.

Art. 21 Traçabilité

[1] Tout traitement de données (création, validation, accès, communication, réception, modification) doit pouvoir être retrouvé facilement, y compris l'identification des personnes ayant participé à ce traitement de données et la date.

[2] La consultation de données en cas d'urgence au sens de l'article 17, alinéa 12, est signalée automatiquement au médecin de confiance, avec mention de la date, de l'heure, du nom du patient et du nom du médecin.

Art. 22 Organe responsable

[1] La Fondation est responsable de la sécurité de la transmission des données.

[2] A ce titre, la Fondation est compétente pour émettre des directives concernant les exigences techniques minimales et la manière de traiter les données.

Art. 23 Secret

[1] Les collaborateurs et organes de la Fondation ainsi que les experts externes auxquels elle recourt sont tenus au secret.

[2] Ils n'ont pas le droit de communiquer ou de mettre à disposition de tiers les informations obtenues dans l'exercice de leurs tâches, sauf s'ils y sont autorisés ou contraints par une autre disposition légale.

Chapitre V Sanctions pénales et administratives

Art. 24 Sanctions pénales

A moins que le code pénal ne prévoie une peine plus lourde, le prestataire de soins, le collaborateur ou l'organe de la Fondation ou l'expert externe, qui aura violé son obligation de garder le secret ou aura accédé à des données pour le traitement desquelles il n'est pas habilité, sera puni des arrêts ou de l'amende.

Art. 25 Sanctions administratives

Les prestataires de soins qui contreviennent intentionnellement ou par négligence aux dispositions de la présente loi sont passibles des sanctions administratives prévues par la loi sur la santé, du … *(date d'adoption)*.

Chapitre VI Dispositions finales et transitoires

Art. 26 Phase pilote et évaluation

[1] Le réseau communautaire d'informatique médicale fait l'objet d'une phase pilote de trois ans.

[2] Il est soumis à une évaluation externe indépendante dans les trois ans qui suivent la phase pilote.

Art. 27 Dispositions d'application

Le Conseil d'Etat édicte les dispositions nécessaires à l'application de la présente loi.

Art. 28 Entrée en vigueur

Le Conseil d'Etat fixe l'entrée en vigueur de la présente loi.

Art. 29 Modifications à une autre loi

La loi sur les informations traitées automatiquement par ordinateur (LITAO), du 17 décembre 1981, est modifiée comme suit :

Art. 9 Accès

Fichiers médicaux

[4] L'accès aux fichiers médicaux est régi par la loi sur la santé, du … *(date d'adoption)*.

Certifié conforme
Le chancelier d'Etat : Robert Hensler

EXPOSÉ DES MOTIFS

Mesdames et
Messieurs les députés,

I. INTRODUCTION

La santé est une des préoccupations principales de la population en Suisse et en particulier à Genève. Bien que le fonctionnement de notre système de santé satisfasse largement la majorité des citoyens et de la classe politique, l'évolution des coûts de la santé menace l'intégrité de ce même système.

Le Conseil d'Etat, afin de préserver les acquis, tout en améliorant la qualité, l'efficience et l'ouverture, a indiqué que l'autorité cantonale devait mettre en place un réseau de soins formé des acteurs publics et privés autorisés à exercer les différentes professions de la santé (rapport au Grand Conseil sur la politique de la santé - RD 281 du 27.08.1997 et rapport au Grand Conseil sur la planification hospitalière du système de santé genevois 2003-2010 - RD 483 du 16.04.2003). Il a confié à la Fondation IRIS-GENÈVE la définition, la réalisation et l'exploitation d'un réseau communautaire d'informatique médicale (RCIM), dont le but est de contribuer durablement à la qualité et à l'efficience du système de santé genevois dans l'intérêt des patients et des professionnels de la santé.

Ce réseau, nommé « *e-toile* », repose sur l'idée que chaque individu, au cours de sa vie, consulte un nombre important de prestataires de soins. Il consulte des médecins, est pris en charge par un hôpital, une clinique ou un EMS, est radiographié suite à un accident, ... autant de situations au cours desquelles ces différents fournisseurs de soins constituent, dans leur dossier, une partie de l'histoire médicale d'un patient.

Le concept proposé est la mise en réseau des différents épisodes de cette histoire et la possibilité, pour les prestataires de soins, d'y accéder depuis leur poste de travail. Ainsi, la constitution d'un dossier médical virtuel complet, dans lequel figure l'ensemble des données thérapeutiques, médicamenteuses ou de soins, aidera les prestataires de soins à faire les bons choix et favorisera le suivi d'un projet de soins cohérent, avec une option thérapeutique claire et lisible. Placé au cœur de ce réseau d'informatique médicale, le patient pourra avoir recours à un ou plusieurs médecins de confiance pour l'aider à gérer son dossier médical décentralisé.

Le projet de loi « *e-toile* », bien qu'ayant un objectif d'élargissement au plan national, mais en l'absence d'une loi-cadre en la matière, nécessite un cadre légal cantonal.

Le présent projet de loi pose ce cadre, nécessaire à l'organisation du réseau e-toile, à l'accès aux données, ainsi qu'au traitement des données et à leur sécurité.

II. LES CONSULTATIONS DE JANVIER 2002, AOÛT 2003 ET LE PRESENT PROJET DE LOI

En date du 2 janvier 2002, une procédure de consultation relative à un avant-projet de loi, « sur l'informatisation des dossiers médicaux et sur la clé électronique des patients », élaboré par la Fondation IRIS, a été lancée par le conseiller d'Etat Pierre-François Unger, chef du département de l'action sociale et de la santé (ci-dessous : DASS). Cette consultation a donné lieu à des commentaires en provenance de 54 groupes, associations, experts, fédérations ou établissements, et a reconduit un travail de réflexion de fond dont le présent projet de loi est le fruit. L'Institut de droit de la santé (ci-dessous : IDS) a également été sollicité, et a apporté sa contribution quant au fond et à la forme du projet de janvier 2002.

Suite à cette procédure de consultation, le chef du DASS a mandaté l'IDS pour analyser les problèmes juridiques relatifs à la mise en place du réseau « *e-toile* ». Un rapport préliminaire a été rendu en automne 2002. Le chef du DASS a ensuite mandaté l'IDS pour élaborer un nouvel avant-projet de loi, en collaboration avec la Fondation IRIS, relatif à l'étape de mise en œuvre du réseau « *e-toile* », dont le cadre temporel a été fixé entre 2005 et 2008. Cette étape est caractérisée par son caractère facultatif, par le rôle central dévolu à la volonté du patient qui conserve une maîtrise sur tous les traitements de données (terme ici employé au sens large, comme dans la loi fédérale sur la protection des données; il comprend donc également la simple consultation des données), par la non-inclusion des assureurs sociaux et par les responsabilités confiées à la Fondation IRIS, chargée de promouvoir et de gérer le réseau. La modification de certains de ces éléments de base (exemple : passage à un caractère obligatoire) nécessitera une adaptation des dispositions légales.

Le 23 juillet 2003, un rapport incluant une analyse comparative de projets analogues, un business plan et une présentation détaillée des options techniques et des travaux nécessaires à un déploiement large du réseau « *e-toile* » a été présenté au Conseil d'Etat.

Au vu de l'étendue et de l'impact d'« *e-toile* » sur le système de santé, le Conseil d'Etat a décidé, après avoir pris connaissance du rapport de juillet 2003, de lancer une procédure de consultation. Cette consultation a permis de déceler les préoccupations principales des acteurs et de soulever un

certain nombre de questions provenant de 68 groupes, associations, experts, fédérations ou établissements.

Le projet de loi, en ce qui le concerne, répond aux attentes et préoccupations des groupes consultés. L'article 8 du projet de loi « Rectification ou effacement de données inexactes » a été complété sur la base d'une étude demandée à un expert indépendant de l'IDS.

Les idées-maîtresses suivantes ont guidé l'élaboration du projet de loi :

– simplicité de la formulation ;
– élaboration d'un texte englobant l'ensemble des aspects de la problématique ;
– garanties de protection des données tout en recherchant le meilleur compromis entre la protection de la personnalité et les possibilités nouvelles offertes par l'introduction d'une carte-santé.

Le projet de loi reflète la volonté de placer le patient au centre du système, par le biais d'autorisations soit spécifiques soit plus générales, exigeant en principe la présence du patient et de sa carte pour la consultation des données. Le patient doit en effet rester maître des informations qui le concernent, en vertu de son droit à l'autodétermination.

Le projet de loi est à notre connaissance le premier en la matière en Suisse. Sa rédaction a été ponctuée par plusieurs discussions réunissant des intervenants de plusieurs disciplines : médecins, informaticiens, politiciens, éthiciens et juristes. Dans la mesure du possible, il a été tenu compte de deux autres projets en Suisse : celui visant l'introduction d'une carte d'assuré LAMal au niveau fédéral, piloté par l'OFAS en collaboration avec l'Institut Santé et Economie, et le projet tessinois visant à introduire une carte santé sur le plan cantonal. Il a également été inspiré d'expériences faites dans d'autres pays, notamment en Europe.

Ce rapport fait partie d'un ensemble de quatre documents relatifs à tous les autres aspects du projet qui sont :

– le rapport du Conseil d'Etat au Grand Conseil relatif à l'étude détaillée du RCIM du système de santé du canton de Genève appelé « *e-toile* »;
– le projet de loi ouvrant un crédit au titre de subvention cantonale d'investissement pour financer la construction et le déploiement du réseau « *e-toile* » du système de santé du canton de Genève";
– le projet de loi relatif aux statuts de la Fondation de droit public IRIS-GENÈVE.

Sont ainsi uniquement commentées ici les dispositions légales proposées, afin d'expliquer certains choix de principe effectués, les dispositions du projet de loi et les motivations qui ont conduit à leur formulation. Le détail de l'ensemble du projet, se trouve dans les documents cités plus haut.

III. STRUCTURE DU PROJET

Le texte du projet de loi est composé de six parties :

- *les dispositions générales (art. 1-8)* : elles comprennent la description du but, les définitions employées, le champ d'application et les principes juridiques relatifs à la protection des données ;
- *l'organisation du réseau (art. 9-15)* : il s'agit des caractéristiques générales du réseau et de son fonctionnement ainsi que de l'explication du rôle spécifique du médecin de confiance ;
- *l'accès aux données et transmission (art. 16-17)* : ces dispositions établissent plusieurs catégories de données, posent le principe de l'accès sélectif et déterminent les personnes qui ont accès à chaque catégorie de données ;
- *la sécurité de la transmission des données (art. 18-23)* : le but de ces dispositions est de poser quelques principes contraignants pour la conception technique du système (cryptage, traçabilité, etc.) et d'astreindre au secret les personnes gérant le réseau ;
- *les sanctions pénales et administratives (art. 24-25)* : deux dispositions portent spécifiquement sur les sanctions encourues ;
- *les dispositions finales et transitoires (art. 26-29)* : elles portent notamment sur la phase pilote, l'entrée en vigueur, et les dispositions d'application.

La structure proposée distingue entre les éléments purement juridiques relatifs à la protection des données, la description contraignante des caractéristiques du système afin de le rendre compatible avec les principes de protection des données et la définition des accès sélectifs accordés aux différents acteurs du réseau, en fonction de catégories de données prédéfinies.

IV. COMMENTAIRE DES DISPOSITIONS DU PROJET

Art. 1 Objet et buts

La loi a pour but premier de régir le réseau communautaire d'informatique médicale en respectant les principes de protection des données et par conséquent la sphère privée des titulaires d'une carte-santé. Celle-ci s'inscrit dans des mesures plus générales visant à améliorer la qualité et l'efficience des soins.

Art. 2 Définitions

Les principaux termes utilisés dans le projet de loi sont définis à l'article 2. Pour faciliter la lecture des dispositions légales, il a été choisi d'employer le terme « patient », tout en restant conscient du fait que chaque titulaire de carte n'est pas forcément un patient, c'est-à-dire une personne en traitement.

La notion de prestataire de soins a été préférée à celle de fournisseur de soins, même si cette dernière correspond à la terminologie utilisée dans la loi fédérale sur l'assurance-maladie. L'élargissement du cercle des prestataires de soins à des unités médicales extra-cantonales avec lesquelles un accord de collaboration a été conclu doit être relevé ici. Cela nécessitera une négociation de certains aspects liés au rattachement au réseau « *e-toile* ».

Le langage technique relatif aux systèmes informatiques n'a pas été introduit, car il aura plutôt sa place dans une directive ou un règlement.

Art. 3 Champ d'application personnel

Cette disposition s'inscrit dans la première étape du processus d'introduction du système « *e-toile* » à Genève et indique le caractère facultatif de l'adhésion à ce système, autant pour les patients que pour les prestataires de soins.

Après avoir hésité à restreindre le champ d'application du projet de loi aux seules personnes physiques majeures, afin d'éviter, pendant la première étape, les questions relatives à l'exercice des droits et au discernement des mineurs et des interdits, il a finalement été retenu une version qui englobe toute personne physique.

Les critères « *habiter ou exercer une activité professionnelle* » ont été préférés à celui du domicile ou à celui d'assuré. Le critère du domicile exclurait un certain nombre de personnes, dont les frontaliers ou une partie du personnel des organisations internationales. Le critère « assuré » nécessiterait une précision (assuré LAMal, assuré LAA, assuré AVS, etc.) et

ferait référence à un lien avec les assurances sociales, qui a justement été écarté dans le cadre de cette première étape du projet.

L'alinéa 2 indique que tout prestataire de soins, au sens défini dans l'article 2, peut demander à adhérer au réseau. La possibilité d'exclure certaines spécialités dans le cadre de cette première étape (par exemple la psychiatrie ou les soins dentaires) a été discutée, mais a finalement été laissée de côté.

Art. 4 Personnes n'ayant pas le plein exercice des droits civils

Cette disposition a paru nécessaire en raison du choix effectué à l'article 3 en faveur d'un champ d'application personnel étendu à toute personne habitant ou exerçant une activité professionnelle dans le canton de Genève. L'article 4, alinéa 1, précise que les mineurs et les interdits capables de discernement peuvent exercer seuls tous les droits reconnus aux patients par le projet de loi, conformément aux principes du droit fédéral applicables aux droits strictement personnels.

Si la personne est incapable de discernement (art. 4, al. 2), les mécanismes de représentation ancrés dans le projet de loi sur la santé s'appliqueront.

Art. 5 Liberté d'entrer et de sortir du réseau

La première étape, telle que prévue dans le projet de loi, est facultative et, de ce fait, caractérisée par la liberté d'adhérer au système, autant pour les prestataires de soins que pour les patients (art. 5, al. 1). Ceci correspond aux recommandations émises par le préposé fédéral à la protection des données (PFPD), en tout cas pour la phase actuelle de la réflexion. Dans une note du 16 décembre 2002 relative au projet d'introduire une carte d'assuré LAMal au niveau fédéral, le PFPD précisait que si des données médicales d'urgence devaient être intégrées à la carte, le système devrait être facultatif.

Le corollaire de cette liberté d'adhésion est la liberté de sortir du réseau. Pour le patient, cela implique qu'il peut décider en principe en tout temps de quitter le réseau, sauf la première année. La seule restriction apportée par le projet de loi consiste à limiter la sortie effective du réseau à la fin d'une année civile (art. 5, al. 2). Les aspects techniques relatifs au sort des données en cas de sortie du patient devront encore être élucidés.

Nous partons de l'idée que, pour les prestataires de soins, l'adhésion au réseau nécessitera des investissements, dont le financement devra encore être déterminé par le Conseil d'Etat (article 13, al. 2). C'est pourquoi nous proposons de limiter la possibilité du prestataire de soins de quitter le réseau

en fixant une durée minimale de trois ans de raccordement au réseau et, là aussi, de limiter la sortie effective à la fin d'une année civile (art. 5, al. 3).

Art. 6 Prohibition de discriminer

Un système facultatif et nécessitant le consentement ponctuel du patient en principe pour chaque traitement de données pourrait conduire à des discriminations en cas de refus du patient d'adhérer ou de consentir à une consultation des données. Il faut éviter que des soins ne soient accordés qu'à condition d'avoir accès à des données médicales que le patient ne voudrait pas dévoiler. L'article 6 veut empêcher les discriminations, en réaffirmant la prohibition de discriminer, déjà ancrée en termes généraux dans la Constitution fédérale (art. 8 Cst.).

La disposition vise non seulement des discriminations touchant le patient, telles que le refus d'accès à certains soins, mais aussi des discriminations frappant le prestataire de soins, comme un refus d'autorisation de pratiquer.

Art. 7, alinéas 1 et 2 Légalité et bonne foi

Nous avons retranscrit en partie, dans l'article 7, les principes généraux de protection des données énumérés dans les articles 4 et suivants de la loi fédérale sur la protection des données (ci-après LPD), afin de permettre la référence à une seule et même loi et de faciliter ainsi la compréhension et la consultation du texte légal à l'usager.

Art. 7, alinéas 3 et 4 Proportionnalité

Le terme « activité thérapeutique » (art. 7, al. 3) doit être pris ici dans un sens large. Il comprend le diagnostic et le traitement, mais aussi les mesures de prévention et de promotion de la santé ainsi que les soins palliatifs.

L'alinéa 4 prévoit une exception : des données préalablement anonymisées (*unlinked anonymous*, c'est-à-dire ne permettant pas de remonter aux personnes) peuvent être utilisées à des fins statistiques. Cette exception n'en est pas vraiment une dès l'instant où l'anonymisation fait perdre aux données leur qualité de données personnelles justifiant leur protection.

Art. 7, alinéa 5 Sécurité des données

Il appartiendra à la Fondation de veiller à adapter régulièrement les exigences de sécurité des données aux derniers développements techniques et informatiques.

Art. 7, alinéa 6 Exactitude des données

Nous avons limité la portée du principe de l'exactitude des données aux seuls actes d'enregistrement et de modification de données. Il serait disproportionné d'exiger le contrôle de l'exactitude chaque fois que le médecin de confiance ou un autre prestataire de soins consulte les données du patient.

Art. 8 Rectification ou effacement des données inexactes

Il s'agit d'un élément fondamental du droit constitutionnel à l'autodétermination informationnelle, qui est repris dans les dispositions légales sur la protection des données personnelles, tant fédérales que cantonales. Cette disposition est dès lors inéluctable (art. 8, al. 1), même si elle présente des difficultés techniques.

Art. 9 Caractéristiques du réseau

Le réseau doit permettre d'accéder, en fonction des droits d'accès et des autorisations données par le patient, à des informations médicales contenues dans les dossiers tenus par d'autres prestataires de soins (art. 9, al. 1).

Il n'a pas pour vocation de créer un dossier virtuel centralisé par patient (art. 9, al. 2). En revanche, il va de soi que le médecin doit avoir la possibilité, comme c'est déjà le cas avec les dossiers papier, de constituer son propre dossier sur le réseau en l'enrichissant d'informations dont il a besoin pour l'épisode de soins. Il peut naturellement aussi faire une copie papier de son dossier. En revanche, l'exportation de données ou le transfert d'un dossier sur un autre support électronique est prohibé. L'idée sous-jacente est d'éviter la mise en relation de dossiers ou de parties de dossiers concernant plusieurs patients, à l'exception des statistiques anonymisées.

Art. 10, alinéas 1 à 3 Médecin de confiance – Rôle

Le réseau prévoit l'introduction d'une nouvelle fonction: celle de médecin de confiance. L'idée est d'accompagner la consultation et l'enregistrement des données ainsi que la définition des niveaux d'accès par les conseils d'un professionnel avec qui le patient a un rapport de confiance particulier (art. 10, al. 1 et 2).

Ce médecin peut être un généraliste ou un spécialiste et n'est pas forcément le médecin traitant du patient. L'option, également préférée par la commission d'éthique accompagnant le projet « *e-toile* », a finalement été prise de permettre au patient d'avoir plusieurs médecins de confiance. Ce dernier n'a dès lors pas de fonction de coordination ou de pivot du système,

mais reste simplement un partenaire privilégié du patient en matière de données médicales, au bénéfice d'un solide rapport de confiance. Au stade actuel, il n'est donc pas question d'en faire le médecin de famille des temps modernes ou le médecin de premier recours qui filtre l'accès aux soins octroyés par des spécialistes ou dans des hôpitaux ou encore le *case-manager* responsable non seulement du traitement, mais également de la gestion économique et du contrôle des soins.

Selon l'article 17, alinéa 13, du projet de loi, le médecin de confiance doit être informé automatiquement de tout accès d'urgence aux données concernant ses patients. Il doit en contrôler le bien-fondé et tenir les renseignements à disposition du patient. De même appartient-il au médecin de confiance d'avertir le patient d'une éventuelle interconnexion du réseau avec un autre réseau (art. 10, al. 3). On sait par exemple que le canton du Tessin développe lui aussi un système analogue.

Art. 10, alinéas 4 et 5 Médecin de confiance – Libre choix

Le principe du libre choix du professionnel de la santé découle du droit fédéral et est explicitement ancré à l'article 44 du projet de loi sur la santé du canton de Genève. La même règle doit valoir pour la détermination du ou des médecins de confiance par le patient (art. 10, al. 4). Elle implique aussi la possibilité de modifier ou de révoquer les choix faits précédemment (art. 10, al. 5).

Art. 11 Registre

Le registre des prestataires de soins rattachés au réseau (art. 11, al. 1), tenu par la Fondation, n'a sa raison d'être que tant que le système est facultatif. Il a pour but de renseigner rapidement et gratuitement les personnes qui souhaitent par exemple choisir un médecin de confiance (art. 11, al. 2).

Dès lors que la Fondation gère le réseau et délivre les clefs d'accès, il est inévitable qu'elle ait connaissance de tous les patients ayant reçu une clé (carte-santé d'accès). Le registre des patients qu'elle détient de ce fait est toutefois strictement confidentiel et ne peut pas être consulté par les tiers (art. 11, al. 3).

Art. 12 Dossier du patient

A titre général, la tenue et la conservation des dossiers de patient par les professionnels de la santé est régie par le projet de loi sur la santé, auquel l'article 12, alinéas 1 et 2 renvoie notamment. L'introduction d'une carte-

santé ne change normalement rien aux principes de tenue d'un dossier médical. En revanche, il sera probablement nécessaire d'harmoniser certaines rubriques et de fixer quelques règles sur la teneur du dossier. Cette question doit encore être approfondie sur le plan technique et fera l'objet de dispositions complémentaires du Conseil d'Etat (voir article 27).

Art. 13 Equipement

Un équipement et des services standards seront déterminés par la Fondation pour tous les prestataires de soins rattachés au réseau (art. 13, al. 1). Des incitatifs d'adhésion au réseau, pourront être prévus (art. 13, al. 2).

Art. 14 Surveillance du réseau

Si la Fondation est responsable de l'exploitation et du fonctionnement du réseau, la surveillance, elle, doit être confiée à un autre organe. C'est finalement un organe indépendant désigné par le Conseil d'Etat qui a été retenu (art. 14, al. 1). Cet organe attachera une attention particulière au respect par le réseau des règles juridiques et éthiques.

Art. 15 Clé d'accès

Une carte-santé servant de clé d'accès personnelle sera délivrée par la Fondation à tout patient qui adhère au réseau. C'est cette clé qui servira de sésame pour la consultation de ses données auprès des prestataires de soins rattachés au réseau.

Art. 16 Catégories de données

Après avoir envisagé plusieurs solutions différentes, notamment une répartition des données en six catégories (données administratives, données administratives d'urgence, données médicales d'urgence, données médicales, données stigmatisantes et données pharmaceutiques) ou en trois catégories (données administratives, données médicales, données stigmatisantes) il a finalement été retenu cinq catégories : les données administratives, les données utilitaires, les données médicales, les données stigmatisantes et les données secrètes.

Créer plusieurs catégories de données a pour but de cerner à l'avance, avec un certain degré de précision, qui aura accès à quelles données, en fonction du niveau de sensibilité des données.

Les *données administratives* correspondent aux données qui circulent déjà actuellement très librement et qui permettent d'identifier le patient et ses assureurs.

Les *données utilitaires* n'existeront que si le patient le veut bien et en a déterminé l'étendue. Il s'agit pour l'essentiel de données qui peuvent être très utiles aux prestataires de soins, soit du point de vue personnel, comme le contenu de directives anticipées, les personnes à aviser en cas d'urgence, soit du point de vue médical, comme des allergies et un traitement ou une affection spécifique.

Les *données médicales* comprennent toutes les données relatives à la santé du patient et aux examens et traitements entrepris. Elles ne seront accessibles aux prestataires de soins qu'avec l'accord spécifique du patient, sauf urgence.

Ensuite, le patient peut décider, le cas échéant après avoir demandé conseil au médecin de confiance, d'attribuer certaines données à la catégorie *données stigmatisantes*, notamment parce que leur révélation pourrait porter une grave atteinte à sa vie privée. Ces données ne seront alors accessibles qu'au seul médecin de confiance.

Enfin, le patient peut décider de tenir des données hors d'atteinte d'autres utilisateurs du réseau, dans une catégorie *données secrètes*.

Art. 17, alinéas 1 à 4 Accès aux données – Principes

Le système est basé sur la nécessité de deux clés d'accès pour accéder aux données : celle du prestataire de soins et celle du patient (art. 17, al. 1). Par l'introduction de la carte dans le lecteur et l'identification par le code, la personne exprime son consentement au traitement des données.

L'alinéa 2 formule la ligne directrice de ce qui doit se faire sur le plan technique: prévoir un accès sélectif aux données, c'est-à-dire déterminer à l'avance qui a accès à quelles données. Son corollaire, à l'alinéa 3, est que les personnes non habilitées ne doivent pas pouvoir accéder aux données. Les aspects techniques, notamment le cryptage, sont réglés dans l'article 18.

Un des problèmes souvent évoqués par la doctrine en matière de protection des données, est la création de fichiers de données personnelles de nombreux patients présentant certaines caractéristiques communes.

L'alinéa 4 a pour but d'empêcher par exemple de produire une liste nominale de tous les patients ayant consulté le dermatologue X ou ayant attrapé la maladie Y. En revanche, il n'empêche pas l'élaboration de statistiques respectant scrupuleusement l'anonymat des patients (cf. art. 7, al. 4).

Art. 17, alinéas 5 à 7 Accès aux données – Par le patient

Le patient peut accéder seul, en tout temps, à ses propres données (art. 17, al. 1), grâce à des bornes spéciales. Comme pour tout autre dossier médical, sont exceptées du droit d'accès les notes purement personnelles et les données concernant exclusivement des tiers, conformément aux prescriptions du projet de loi sur la santé.

Comme un dossier médical n'est pas toujours d'une lecture aisée, l'article 17, alinéa 6, prévoit que le patient a le droit de se faire expliquer ses données par un médecin de confiance. Ce dernier devra le recevoir dans un délai raisonnable, lui fournira les explications requises et vérifiera qu'il a bien compris (art. 17, al. 7).

Art. 17, alinéas 8 et 9 Accès aux données – Par le médecin de confiance

De tous les prestataires de soins, le médecin de confiance a l'accès le plus large aux données du patient, y compris aux données stigmatisantes, mais en présence du patient et avec la clé d'accès de ce dernier (art. 17, al. 8).

Ce n'est que sur la base d'une autorisation spéciale du patient que le médecin de confiance pourra également avoir cet accès en l'absence du patient (art. 17, al. 9), par exemple pour se préparer à la consultation.

Art. 17, alinéas 10 et 11 Accès aux données – Par les autres prestataires de soins

Tout prestataire de soins (donc y compris les médecins de confiance) ont accès en tout temps, avec leur seule clé, aux données administratives du patient et aux données utilitaires que le patient aura éventuellement déterminées (art. 17, al. 10).

La logique du système veut que l'accès aux autres données par les prestataires de soins qui ne sont pas des médecins de confiance soit plus restreint. Les prestataires de soins ne peuvent pas consulter les données stigmatisantes ni l'ensemble des données médicales, mais seulement celles qui sont nécessaires à sa mission dans l'épisode de soins (art. 17, al. 11).

Bien entendu, les prestataires de soins peuvent accéder en tout temps au dossier qu'ils ont eux-même établi, comme c'est le cas actuellement.

Art. 17, alinéas 12 et 13 Accès aux données – En cas d'urgence

Lorsqu'un incendie débute, il faut assurer la sortie des personnes qui se trouvent dans l'objet en flammes. Souvent, il s'agit de briser une vitre pour sortir ou pour avoir accès à une clef. C'est ce principe qui a été choisi ici.

Lorsque la vie ou la santé du patient sont menacées d'un danger imminent, chaque médecin rattaché au réseau doit pouvoir, grâce à sa seule clé, consulter les données médicales (mais pas les données très sensibles) du patient (art. 17, al. 12) sans devoir chercher d'abord si le patient porte sa clé d'accès sur lui et s'il peut éventuellement formuler des bribes de consentement. Bien entendu, on ne peut briser la vitre que si l'identité du patient reçu en urgence est connue.

Cet accès d'urgence, qui constitue une intrusion importante dans la sphère privée du patient, même si elle est en principe effectuée dans l'intérêt de celui-ci, est limité aux prestataires de soins médecins. En effet, on peut partir de l'idée que, même s'il n'y a que des ambulanciers sur place, ceux-ci seront en lien avec un service d'urgences hospitalier et donc un médecin.

Chaque vitre brisée est, à des fins de contrôle, automatiquement signalée au médecin de confiance. Il a paru préférable de décentraliser ce contrôle plutôt que de le confier à la Fondation, en raison du nombre potentiellement important de cas. Le patient a accès en tout temps au journal comprenant tous les accès à ses données (art. 17, al. 13).

Art. 18 Cryptage

Il s'agit de l'aspect technique de l'accès sélectif aux données. Le cryptage doit correspondre au meilleur standard disponible en Suisse (art. 18, al. 1). Ceci implique une adaptation régulière à ce standard. C'est pourquoi, nous proposons que les détails soient réglés par la Fondation (art. 18, al. 2) qui, par ailleurs, est l'organe responsable de la sécurité de transmission des données (cf. art. 22, al. 1).

Art. 19 Identification personnelle

La clé n'est pas encore un élément suffisant pour exprimer le consentement du patient (elle peut être volée par exemple). Elle n'est qu'un instrument servant à l'identification de la personne, notamment si elle est complétée par une photo. Mais c'est l'utilisation du système d'identification personnelle, par le biais d'un code d'identification personnel (NIP) qui exprimera le consentement du patient à un traitement des données par tel prestataire de soins.

Art. 20 Attestation de réception

Il s'agit d'un moyen de contrôler que les informations dont la consultation était sollicitée sont arrivées auprès du bon destinataire.

Art. 21 Traçabilité

Tout traitement des données doit pouvoir être reconstitué sur la base du nom des prestataires de soins et des patients, ainsi que des dates précises (art. 21, al. 1). Toute consultation en cas d'urgence est automatiquement signalée au médecin de confiance avec les mêmes précisions (art. 21, al. 2).

Art. 22 Organe responsable

La sécurité de la transmission des données est de la responsabilité de la Fondation (art. 22, al. 1) qui peut émettre des directives dans ce domaine (art. 22, al. 2).

Art. 23 Secret

L'alinéa 1 prévoit d'étendre l'obligation de garder le secret (qui pèse sur tous les prestataires de soins) aux collaborateurs et organes de la Fondation ainsi qu'aux experts externes qu'elle s'adjoindra. L'obligation sera absolue, à moins qu'une disposition légale ne permette ou ne contraigne ces personnes à révéler certaines informations (art. 23 al. 2). La violation de cette obligation est sanctionnée pénalement (art. 24). Les membres de la Fondation sont également soumis à l'obligation de secret découlant de l'article 6 LITAO.

Art. 24 Sanctions pénales

Tout accès non autorisé à des données de même que toute violation de l'obligation de garder le secret au sens de l'article 23 pourra faire l'objet de sanctions pénales (arrêts ou amende).

Art. 25 Sanctions administratives

L'expérience montre que des sanctions administratives peuvent parfois être plus dissuasives que des sanctions pénales. C'est pourquoi l'article 25 prévoit que les sanctions administratives prévues par le projet de loi sur la santé pourront aussi être prises à l'encontre d'un prestataire de soins qui aura contrevenu à la présente loi.

Art. 26 Phase pilote et évaluation

Etant donné que l'introduction d'une « carte santé » donnant accès à des données médicales est une innovation en Suisse, il est prévu de procéder par étapes. La première étape, régie par la présente loi, est facultative pour les patients et pour les prestataires de soins et exclut la participation des assureurs sociaux. Cette phase pilote durera trois ans (art. 26, al. 1) à partir du début de la phase opérationnelle.

Cela semble être un minimum si l'on veut pouvoir en tirer des leçons. C'est pourquoi l'alinéa 2 impose une évaluation externe indépendante qui devra être faite au plus tard dans les trois ans suivant la phase pilote.

Rappelons que si la participation des assureurs sociaux était souhaitée, il faudrait transposer le système au niveau national, puisque les compétences en matière d'assurances sociales appartiennent à la Confédération.

Art. 27 Dispositions d'application

Il appartiendra au Conseil d'Etat d'édicter les dispositions nécessaires à l'application de la présente loi.

Art. 28 Entrée en vigueur

Il appartiendra au Conseil d'Etat de la fixer.

Art. 29 Modifications à une autre loi

La présente loi a déjà pris en compte le projet de loi sur la santé. Si ce dernier n'entrait pas en vigueur simultanément, il faudra prévoir quelques adaptations de dispositions légales en vigueur. Une vérification systématique devra être faite le moment venu.

Au bénéfice de ces explications, nous vous remercions, Mesdames et Messieurs les députés, de réserver un bon accueil au présent projet de loi.