Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

GDK Schweizerische Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren
CDS Conférence suisse des directrices et directeurs cantonaux de la santé
CDS Conferenza svizzera delle direttrici e dei direttori cantonali della sanità

Cybersanté Suisse

Rapport final du projet partiel « Bases légales »

Approuvé par le comité de pilotage

Berne, le 20 août 2009

ehealthsuisse
Koordinationsorgan Bund-Kantone
Organe de coordination Confédération-cantons
Organi di coordinamento Confederazione-Cantoni

Impressum

Organisation du projet : Comité de pilotage : Pascal Couchepin (conseiller fédéral, chef du DFI, présidence), Thomas Zeltner (directeur de l'OFSP), Peter Indra (vice-directeur de l'OFSP), Stefan Spycher (vice-directeur de l'OFSP), Carlo Conti (conseiller d'Etat, directeur de la Santé, BS), Markus Dürr, conseiller d'Etat, directeur de la Santé, LU), Heidi Hanselmann (conseillère d'Etat, directrice de la Santé, SG), Patrizia Pesenti (conseillère d'Etat, directrice de la Santé, TI).

Comité de direction du projet : Adrian Schmid (secrétariat eHealth Confédération-cantons, présidence), Pia Ernst (OSP), Andreas Faller (Santé BS), Catherine Gasser (OFSP), Hansjörg Looser (Santé SG), Andrea Nagel (OFSP), Georg Schielke (CDS), Hans-Peter Schönenberger / Felix Schneuwly (santésuisse), Christoph Schöni / Caroline Piana (H+), Michael Stettler (OFSP), Walter Stüdeli (IG eHealth), Therese Stutz (OFSP), Judith Wagner (FMH).

Membres du projet partiel « Bases légales »: Andreas Altermatt (santésuisse, dès juillet 2008), Thomas Casanova (PRIVATIM), Irène Costis-Droz (DES, GE), Isabelle Gioielli (OFSP), Andreas Hugi (IG eHealth), Hanspeter Kuhn (FMH), Federica Liechti (OFSP), Rolf Lüthi (Cliniques privés suisses), Thomas Meier (PFPDT, dès décembre 2008), Andrea Nagel (OFSP, coresponsable), Kathrin Reichenbach (GEF BE, dès novembre 2008), Georg Schielke (CDS, coresponsable), Urs Stromer (IG eHealth), Stefan Wyss (Comité de direction de la cybersanté Confédération–cantons, secrétariat scientifique).

Autres informations et source :
www.e-health-suisse.ch

Objet et position du présent document

Le comité de pilotage de la Confédération et des cantons pour la mise en œuvre de la Stratégie suisse en matière de cybersanté a donné le 10 avril 2008, les mandats de six projets partiels. Il a adopté le 19 mars 2009 les premières recommandations, celles du projet partiel « Normes et architecture » (voir annexe).

Les recommandations relatives aux cinq autres projets partiels et résumées dans le présent document ont été adoptées le 20 août 2009 par le comité de pilotage. Les couleurs de la trame des recommandations ont la signification suivante :

➢ *les recommandations sur fond vert ont été adoptées à titre définitif. Les acteurs concernés sont invités à les mettre en œuvre.*	*Adoption définitive*
➢ les recommandations sur fond jaune ont été approuvées à titre informatif. L'approbation est assortie du mandat d'approfondir le sujet sur la base des recommandations (Confédération, cantons ou organe de coordination avec d'autres acteurs).	Approbation et mandat d'approfondir

Pour faciliter la lecture du document, la forme générique est utilisée pour désigner les deux sexes.

Sommaire

Résumé

1 Projet partiel « Bases légales »

1.1 Contexte

Résumé du rapport final

Ce chapitre est un résumé du rapport final du groupe de projet partiel « Bases légales » du 20 août 2009. Le rapport est accessible à l'adresse www.e-health-suisse.ch.

Mandat du projet partiel « Bases légales » du 10 avril 2008

Le comité de pilotage de l'organe de coordination de la cybersanté a chargé le projet partiel « Bases légales », le 10 avril 2008, de lui fournir d'ici avril 2009 [mandat ultérieur : d'ici août 2009] un rapport contenant les éléments suivants :

- analyse des conditions cadre juridiques dans les pays comparables et analyse des études internationales avec un résumé concernant la Suisse ;
- catalogue des thèmes à régler sur le plan légal ;
- variantes de la délimitation entre la Confédération et les cantons.

L'adoption du rapport par le comité de pilotage en août 2009 sera précédée par une large audition.

Les recommandations sont des décisions prises à la majorité

Les recommandations formulées ici sont des décisions prises à la majorité par le projet partiel « Bases légales » et, pour une part, par le comité de pilotage (séance du 22 janvier 2009).

Concentration sur deux processus principaux conformément au projet partiel « Normes et architecture »

Conformément aux recommandations du projet partiel « Normes et architecture », l'introduction du dossier électronique du patient se concentre, dans une première phase, sur le domaine des processus cliniques entre fournisseurs de prestations, parmi lesquels deux processus principaux sont jugés prioritaires :

- l'échange d'informations au long de la chaîne de traitement ;
- la prescription intégrée de médicaments.

Ces processus sont à comprendre comme les premières étapes de l'introduction du dossier électronique du patient et ils n'impliquent pas nécessairement pour les fournisseurs de prestations, à ce stade, la tenue d'une fiche clinique électronique.

1.2 Analyse de la situation

Méthode suivie pour l'analyse de la situation

Les champs thématiques suivants ont été sélectionnés et examinés en vue d'obtenir une vue d'ensemble équilibrée des bases légales dans le domaine de la cybersanté : législation dans un choix de pays, effets des bases légales sur les activités relevant de la cybersanté dans un choix de pays, recoupements avec la cybersanté dans la législation nationale et dans les législations cantonales, état de la législation dans les cantons, état de la recherche.

Diversité des bases juridiques

Il est apparu que, tant au plan national qu'international, il existe peu de bases légales sur lesquelles on pourrait s'appuyer pour l'introduction du dossier électronique du patient en Suisse. L'inscription du thème dans la loi a été résolue de manière très différente selon les systèmes juridiques, quand elle l'a été.

Réglementation sans effet sur les techniques

L'analyse de la législation relative à la cybersanté dans un choix de pays a mis en évidence qu'aucun pays n'a édicté de loi spécifique. Les règles appliquées pour la mise en œuvre d'instruments de cybersanté, les devoirs professionnels par exemple, sont rédigées en termes neutres du point de vue des techniques. Elles s'appliquent quelle que soit la manière dont se déroulent les processus d'affaires ou la gestion des dossiers, et donc naturellement aussi lorsque cela se fera à l'avenir, entièrement ou partiellement, par informatique. Là où la question de la communication électronique l'exige, il faudra selon toute probabilité édicter des dispositions visant spécifiquement la cybersanté.

Importance primordiale de la protection des données

La législation sur la protection des données doit aussi être respectée lorsque l'on a recours aux TIC. La protection de la personnalité joue ici un rôle primordial. La majorité des pays étudiés a adopté des dispositions sévères en matière de protection et de sécurité des données pour le traitement et la consultation de données sensibles dans le domaine de la télémédecine et du dossier électronique du patient.

L'identification et l'authentification sont des thèmes importants

L'identification et l'authentification sans ambiguïté des patients et des fournisseurs de prestations sont des conditions indispensables aux applications de la cybersanté.

Il est recommandé de fonder une organisation responsable

Dans presque tous les pays qui ont déjà introduit des applications de cybersanté, un organe de coordination de ce domaine a été fondé. Les tâches de ces organes sont diverses, mais elles comprennent presque sans exception l'évaluation et la surveillance du respect des normes techniques déclarées obligatoires sur recommandation des organisations responsables.

1.3 Description du besoin d'intervention

Méthode suivie pour l'analyse du besoin d'intervention

Les champs thématiques suivants ont été étudiés pour se faire une idée du besoin d'intervention dans le domaine du droit : responsabilité de l'organe de coordination de la cybersanté, dossier électronique du patient, protection et sécurité des données, droits et obligations des patients et des fournisseurs de prestations avant tout, identification, authentification et autorisation. Des réflexions touchant la responsabilité, la surveillance, le financement, les mesures et les sanctions ont aussi été faites.

Principe : légèreté de la législation

Le but visé est de prescrire aussi peu que possible, mais de régler autant que nécessaire. Les bases légales doivent se focaliser sur les personnes concernées (patients, utilisateurs), mais aussi permettre au système de continuer à se développer. Il faut pour cela que les dispositions soient formulées de manière très ouverte. Il s'ensuit que les diverses applications ne peuvent être réglées dans la loi que dans leurs grandes lignes.

Créer un organe de coordination

La création d'une organisation responsable de la cybersanté selon l'exemple international paraît judicieuse en Suisse aussi. Elle doit être inscrite dans la loi.

Inscription dans la loi du dossier électronique du patient

La création de bases légales assurant le succès de la mise en œuvre de la stratégie comprend notamment l'inscription dans la loi du dossier électronique du patient. Celle-ci préparera aussi le terrain pour d'autres applications de la cybersanté.

Carte d'assuré

Il est probable que le développement d'applications de cybersanté déjà introduites par l'ordonnance sur la carte d'assuré (OCA) se poursuivra

dans le cadre du projet Cybersanté. Il faut donc examiner s'il y a lieu d'adapter les dispositions correspondantes de l'OCA. Au cas où la carte d'assuré serait perfectionnée pour servir de clé d'accès au dossier électronique du patient, il faudrait inscrire dans la loi la séparation des fonctions carte d'assuré (purement administrative) et carte de santé (accès à des informations médicales).

Protection et sécurité des données

En Suisse, la protection et la sécurité des données sont réglées dans la loi fédérale et les lois cantonales sur la protection des données. Les dispositions de ces lois sont formulées de façon générale et abstraite. Elles devront être concrétisées et, le cas échéant, adaptées pour le domaine de la cybersanté. Il se justifiera de les rendre plus sévères sur certains points (p. ex., le maniement de données sensibles relatives aux patients) ou d'adapter suivant les cas les lois spéciales, afin de ne pas empêcher d'emblée certaines utilisations.

Identification, authentification et autorisation, trois conditions essentielles

La sécurité dans l'identification et l'authentification des participants au système, ainsi que leur autorisation à consulter ou traiter les données des patients, sont d'une extrême importance. Selon toute vraisemblance, la définition de règles claires en la matière favorisera considérablement l'acceptation de l'ensemble du système par tous les participants.

- Les règles relatives à l'identification des participants au système comprennent les éléments de l'identité numérique, les exigences de qualité auxquelles doit satisfaire cette identité, le service qui délivre les certificats et les modalités du processus d'enregistrement.
- Pour l'authentification, la nécessité de l'authentification, la technique d'authentification, le service qui délivre les certificats et les modalités du processus d'enregistrement doivent être définis.
- Les dispositions relatives à l'autorisation porteront sur les droits d'accès des différents participants au système en fonction de leur rôle, l'étendue du traitement des données, l'historique des accès et les droits de représentation. Il faut également prévoir le droit des fournisseurs de prestations d'accéder aux données en cas d'urgence.

Autres thèmes

La mise en œuvre de la stratégie suisse en matière de cybersanté impliquera le cas échéant d'inscrire d'autres thèmes dans la loi, p. ex., des règles touchant la surveillance, le financement de l'organe de coordination, d'autres applications de cybersanté et prestations de service, la création d'incitations à la certification, les mesures et sanctions, etc.

1.4 Solutions proposées

Manière de procéder : selon le besoin d'intervention

La recherche de solutions se concentre avant tout sur les thématiques suivantes : répartition des compétences entre la Confédération et les cantons et coordination au sein de l'Etat ; responsabilité de l'organe de coordination de la cybersanté ; inscription dans la loi du dossier électronique du patient et d'autres applications ; protection et sécurité des données ; droits et obligations ; identification, authentification et autorisation ; ainsi que d'autres thèmes tels que responsabilité civile, surveillance, financement, mesures et sanctions ou règles de procédure.

Répartition des compétences entre la Confédération et les

Il est vite apparu clairement que la recherche de solutions pour les thèmes où un besoin d'intervention avait été identifié serait fortement dominée par la décision de principe relative à la répartition des compétences entre la

Confédération et les cantons. C'est pourquoi les deux thèmes suivants ont été déclarés prioritaires : cantons

- répartition des compétences entre la Confédération et les cantons pour la mise en œuvre de la stratégie suisse de cybersanté ;
- formes de coordination nationale dans le domaine de la mise en œuvre de la stratégie suisse de cybersanté.

Diverses possibilités d'inscription dans le droit fédéral (du dossier électronique du patient en particulier) ont en outre été élaborées et l'on a examiné qui pourrait assumer à l'avenir la responsabilité de l'organe de coordination. Des résultats intermédiaires sont disponibles pour l'authentification et l'autorisation.

1.4.1 Recommandation relative à la répartition des compétences entre la Confédération et les cantons

- Recommandation 1 : Il est recommandé à la Confédération de mettre en œuvre la stratégie Cybersanté en épuisant au maximum les compétences juridiques existantes au niveau fédéral. Il faudra se prononcer sur l'éventualité d'une modification de la Constitution dans le cadre des travaux législatifs. — Epuiser les compétences au niveau fédéral avec une éventuelle modification de la Constitution

Le comité de pilotage Cybersanté, à sa séance du 22 janvier 2009, a recommandé de mettre en œuvre la stratégie en recourant le plus possible aux compétences sur le plan fédéral, afin de mettre en place une réglementation aussi unitaire que possible.

Des compétences fédérales qui pourraient servir de base existent en particulier dans les domaines de l'assurance-maladie et accidents (art. 117 Cst.), de la protection de la santé (art. 118 Cst.) et de l'activité économique lucrative privée (art. 95 et 122 Cst.). La gestion d'un dossier électronique du patient de grande envergure, que vise la stratégie en matière de cybersanté, ne peut toutefois pas être dérivée de façon générale de ces bases constitutionnelles, car les compétences fédérales en question sont lacunaires. Le dossier électronique du patient sert d'abord à la fourniture des soins, qui est du ressort des cantons.

1.4.2 Recommandation relative à la coordination nationale

- Recommandation 2 : Les cantons complètent les bases légales nécessaires dans le cadre de leurs compétences pour combler les lacunes dans la réglementation fédérale qui résulteraient inévitablement du partage des compétences. Il leur est recommandé de coordonner les efforts en matière de législation cybersanté. — Combler les lacunes juridiques par une action coordonnée des cantons

Il faudrait que les cantons comblent de manière uniforme les lacunes qui subsistent dans le droit fédéral, (a) en chargeant de cette tâche un organe intercantonal (conformément à l'art. 48 Cst.), (b) en créant un droit intercantonal au moyen d'un concordat fixant des règles de droit directement ou (c) indirectement, ou (d) en coordonnant les procédures législatives cantonales correspondantes via la CDS. La CDS peut élaborer des recommandations à l'intention des cantons et mettre à disposition des textes types pour l'édiction de dispositions légales par les cantons. Le canton de Genève, qui dispose déjà d'une base juridique spécifique à la cybersanté, a incité, dans le cadre de l'audition, les cantons à mettre à disposition un jeu de réglementations-modèles qui puissent être intégrées dans la législation cantonale.

1.4.3 Recommandation relative à l'inscription du dossier électronique du patient dans le droit fédéral

Recommandation 3 : Il est recommandé à la Confédération de promulguer des réglementations en vue de la création de bases légales concernant le dossier électronique du patient. La décision concernant la structure formelle de ces réglementations légales pour le dossier électronique du patient au niveau fédéral (nouvelle loi-cadre / actes modificateurs / modification d'une loi avec adaptations d'autres lois) doit être prise après la première phase des travaux législatifs.	Bases légales

Le projet partiel « Bases légales » prévoyait à l'origine la promulgation d'une loi-cadre. Etant donné l'étroitesse des compétences que la Constitution fédérale accorde à la Confédération dans le domaine de la santé, il devrait être difficile de justifier la promulgation d'une nouvelle loi fédérale autonome. Cependant, l'édiction d'une « loi-cadre sur la cybersanté » présenterait aussi des avantages significatifs, en mettant en évidence l'importance de la cybersanté. Les règles relatives à l'ouverture, à la gestion et à l'entretien du dossier électronique du patient seraient ainsi clairement séparées de l'application des assurances sociales. Tous les assureurs sociaux seraient visés de la même manière en tant qu'agents financeurs, ce qui ne serait pas le cas, par exemple, en cas de fixation de ces règles dans la LAMal. Cela permettrait aussi d'inclure dans la loi les règles relatives à un portail de la santé, au contenu d'un tel portail, et plus tard aussi d'autres aspects ou applications du domaine de la cybersanté. Une loi conçue comme une loi-cadre réglerait notamment les principes essentiels et les principales conditions cadre, ce qui correspond exactement à la philosophie de base adoptée (voir chap. 4.3 du rapport final).

Après l'audition de mai/juin 2009, les recommandations 1 et 3 ont été reformulées notamment en raison des indications exhaustives de l'Office fédéral de la santé publique (OFSP) et des prises de position de différents cantons. L'OFSP, qui dirigera le prochain projet législatif, prendra ultérieurement des décisions essentielles comme une modification éventuelle de la Constitution et la structure formelle des réglementations légales. Les adaptations effectuées ont permis d'éliminer les divergences entre les recommandations 1 et 3. Leur impact se réduit à la recommandation de promulguer des réglementations fédérales.

1.4.4 Recommandation relative à l'identification des patients

Recommandation 4 : Dans les autres travaux visant la mise en œuvre de la stratégie, il faut clarifier s'il est souhaité que le numéro AVS soit utilisé pour l'identification des patients. En cas d'avis favorable, il est recommandé à la Confédération d'envisager une base légale nationale pour utiliser ce numéro comme identifiant du patient, sans toutefois qu'il ne soit l'unique identifiant.	Disposition fédérale pour l'utilisation du numéro AVS comme numéro d'identification des patients

L'utilisation du numéro AVS en tant qu'identifiant du patient est possible à condition de créer de nouvelles bases légales au niveau des cantons ou de la Confédération. Il est cependant délicat d'étendre le but de l'utilisation et le champ d'application de numéros identifiants. Le champ d'application du numéro d'assuré AVS a déjà été considérablement étendu dans le cadre du projet d'harmonisation des registres. Cet élargissement a été fortement controversé et combattu notamment par des arguments invoquant la protection des données. D'un autre côté, le potentiel du numéro AVS en tant qu'« identifiant administratif de personnes »

(« numéro de citoyen ») est aujourd'hui réalité, et son utilisation en tant qu'identifiant du patient ne ferait pas autre chose que tirer parti de ce potentiel. Ce sera aux travaux futurs d'établir s'il est utile et judicieux de prévoir le numéro d'assuré AVS comme identifiant unique pour l'ensemble du système, ou comme un identifiant parmi d'autres.

1.4.5 Recommandation concernant l'examen des mesures de la CE (télémédecine)

La télémédecine n'est pas un champ d'action prioritaire dans la stratégie cybersanté Suisse, mais celle-ci en tient compte comme d'un sous-domaine de la cybersanté à l'instar d'autres processus.

Les projets partiels « Bases légales » ainsi que « Financement et mesures d'incitation » ont cependant abordé le thème de la télémédecine et ont formulé des recommandations. Elles devront être approfondies et adaptées dans les travaux ultérieurs. Il convient de définir ce que l'on entend exactement par « télémédecine », puis de trouver les voies de financement et d'examiner les mesures d'incitation.

- Recommandation 5 : Il est recommandé à la Confédération et aux cantons d'examiner la mise en œuvre, selon leur domaine de compétences, des mesures publiées par la Commission européenne (cf. recommandation 10 du projet partiel Financement et mesures d'incitation).

Examen de la mise en œuvre des mesures de la CE (télémédecine)

La Commission européenne (CE) a publié le 4 novembre 2008 une communication concernant l'utilité de la télémédecine pour les patients, les systèmes de santé et la société. Elle y commente les dispositions relatives aux termes employés et propose des mesures de promotion de la télémédecine. Les Etats membres sont instamment priés :

- d'évaluer leurs besoins et leurs priorités dans le domaine de la télémédecine d'ici à la fin de 2009. Ces priorités devraient faire partie des stratégies nationales de santé qui seront examinées lors de la conférence ministérielle sur la santé en ligne de 2020 ;
- d'examiner et d'adapter d'ici à la fin de 2011 leurs réglementations nationales de manière à ce qu'elles permettent un accès plus large aux services de télémédecine. Elles devront aussi couvrir des aspects tels que l'accréditation, la responsabilité, le remboursement, la confidentialité et la protection des données.

La Commission entend aussi encourager des mesures prises par ses Etats membres et prendre elle-même des mesures. Elle veut notamment instituer une plateforme d'échange sur les réglementations nationales en vigueur et soutenir l'élaboration de lignes directrices en vue d'évaluer les effets, l'efficacité et l'efficience des services de télémédecine.

1.5 Conclusions et perspectives

Les considérations qui précèdent permettent de tirer les conclusions suivantes :

Le processus législatif peut être mis en route au niveau national

- L'interprétation extensive des compétences fédérales recommandée par le comité de pilotage, avec le comblement des lacunes juridiques par une action coordonnée des cantons, offre un garde-fou. Il s'agit maintenant de préparer l'inscription du dossier électronique du patient dans la loi de telle sorte qu'il subsiste le moins possible de lacunes ju-

ridiques.

- Les résultats présentés et les recommandations adoptées permettent à la Confédération d'entamer le processus législatif au niveau national. Les résultats détaillés du projet partiel « Normes et architecture » seront toutefois nécessaires pour les dispositions au niveau des ordonnances.
- Un large appui politique est nécessaire au-delà du cercle des experts en cybersanté.
- Les prochaines étapes des travaux résultent des recommandations formulées. Il conviendra de redéfinir en partie les compétences relatives aux travaux ultérieurs.

2 Contexte

2.1 Mandat et convention de projet

Le Conseil fédéral a approuvé la Stratégie nationale en matière de cybersanté (*eHealth*)[1] le 27 juin 2007. Trois champs d'activité ont été définis : le dossier électronique du patient, les services en ligne et l'application de la stratégie. Comme mesure prioritaire, un organe national de coordination a été créé le 6 septembre 2007. Dans une convention-cadre, le Département fédéral de l'intérieur (DFI) et la Conférence suisse des directrices et directeurs cantonaux de la santé (CDS) ont décidé de s'atteler à l'application de la stratégie. Un secrétariat coordonne les travaux de la Confédération et des cantons.

Adoption de la Stratégie nationale en matière de cybersanté et création de l'organe de coordination Confédération-cantons en 2007

L'objectif C3 de la Stratégie en matière de cybersanté est formulé ainsi :

- *Fin 2008, les questions juridiques encore en suspens sont réglées, les processus législatifs nécessaires à la réalisation des objectifs de la stratégie engagés au niveau fédéral et cantonal, selon les compétences respectives.*

Prescriptions de la Stratégie en matière de cybersanté

Une importance particulière a été reconnue à cet objectif par la formulation d'une deuxième mesure prioritaire dans la stratégie (chap. 9.2 « Préparation de bases légales »). Il y est également fait mention de la motion Noser « E-Health. Utilisation des moyens électroniques dans le domaine de la santé » (04.3243), que les Chambres fédérales ont transmise en mars 2007. Le Conseil fédéral y est chargé de présenter au Parlement un projet de loi sur ce thème.

Le comité de pilotage de l'organe de coordination de la cybersanté a adopté lors de sa première séance, le 10 avril 2008, les mandats des six projets partiels, dont celui du projet partiel « Bases légales ». Ce dernier est chargé de lui fournir d'ici avril 2009 un rapport contenant les éléments suivants :

Mandat du projet partiel « Bases légales » du 10 avril 2008

- *analyse des conditions cadre juridiques dans les pays comparables et analyse des études internationales avec un résumé concernant la Suisse (analyse de la situation) ;*
- *catalogue des thèmes à régler sur le plan légal ;*
- *variantes de la délimitation entre la Confédération et les cantons.*

Ce mandat a été précisé dans la convention de projet du 26 mai 2008, qui définit jalons, ressources et organisation du projet.

Convention de projet du 26 mai 2008

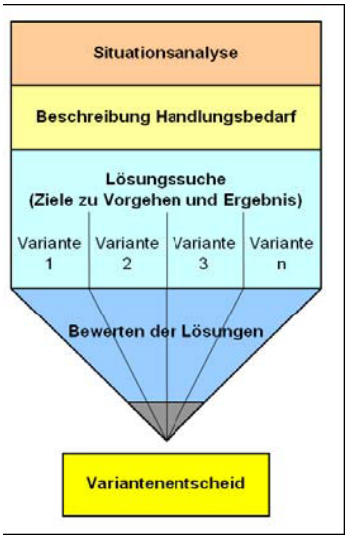
2.2 Démarche

Pour que les recommandations du comité de pilotage soient compréhensibles pour les profanes, il faut, selon le mandat du 10 avril 2008, qu'elles se présentent comme suit :

Prescriptions du mandat du 10 avril 2008

((légende))

[1] La stratégie nationale en matière de cybersanté et d'autres documents peuvent être téléchargés à l'adresse www.ehealth.admin.ch.



Analyse de la situation

Description du besoin d'intervention

Recherche de solutions (objectifs concernant la démarche et les résultats)

Evaluation des solutions

Décision concernant les variantes

Une analyse de la situation dans les champs thématiques concernés est disponible pour la deuxième séance du comité de pilotage en août 2008.

Analyse de la situation

Le besoin d'intervention est tiré au clair d'ici la troisième séance du comité de pilotage en octobre 2008.

Clarification du besoin d'intervention

Des variantes d'application de la stratégie sont présentées au comité de pilotage lors de sa cinquième séance, en mars 2009.

Formation de variantes

Suit une phase durant laquelle le groupe de projet partiel, le groupe d'accompagnement consultatif, les experts éventuellement consultés et les milieux intéressés évaluent les variantes (audition mai/juin 2009).

Evaluation

En août 2009, le comité de pilotage décide de la forme à donner aux conditions cadre légales et recommande ainsi à la Confédération et aux cantons de lancer leurs processus législatifs. Les évaluations sont regroupées dans un rapport final sur l'ensemble des projets partiels.

Décision du comité de pilotage

2.3 Délimitation

Le projet partiel « Bases légales » ne s'occupe pas de l'organisation concrète des systèmes de cybersanté dans d'autres pays. Ces informations ne sont présentées que lorsqu'elles sont importantes pour la compréhension des bases légales.

Délimitation thématique

Le projet partiel ne s'occupe pas non plus de l'établissement de bases légales pour l'utilisation de la carte d'assuré dans des essais pilotes cantonaux, bien que les activités dans ce domaine soient présentées dans l'analyse de la situation des législations cantonales. Le centre d'intérêt du présent rapport dépasse les applications de la carte d'assuré. L'objectif prioritaire n'est donc pas de donner aux cantons des recommandations d'action touchant la législation existante sur la carte d'assuré (art. 42*a* LAMal) (voir PP « Essais pilotes et PPP »[2]).

Délimitation d'avec d'autres projets partiels de la Stratégie nationale en matière de cybersanté

Aucune recherche fondée n'a par ailleurs été menée concernant le financement des infrastructures et des applications de cybersanté. Ces recherches seront menées et présentées dans le cadre du projet partiel « Financement et mesures d'incitation ».

[2] Partenariats public-privé.

3 Analyse de la situation

3.1 Démarche

Les champs thématiques suivants ont été sélectionnés et examinés sous forme de « paquets » en vue d'obtenir une vue d'ensemble équilibrée des bases légales en matière de cybersanté (état au 31 juillet 2008) :

Démarche : diviser le travail en une série de « paquets »

Thème	Question	Chapitre
Législation dans un choix de pays	Comment la cybersanté s'inscrit-elle dans la loi dans d'autres pays ? Expériences / recommandations ?	3.2
Effets des bases légales sur les activités relevant de la cybersanté dans un choix de pays	Quelles bases légales ont fait leurs preuves à l'étranger du point de vue de l'application, lesquelles sont moins concluantes ?	3.3
Recoupements avec la cybersanté dans la législation nationale	Quels textes de loi sont potentiellement pertinents pour l'ancrage légal de la cybersanté ? Quelles bases légales existent déjà ?	3.4
Recoupements avec la cybersanté dans les législations cantonales	Quels textes de loi cantonaux sont potentiellement pertinents pour l'ancrage légal de la cybersanté ? Quelles bases légales existent déjà ?	3.5
Etat de la législation dans les cantons	Quels cantons ont déjà inscrit la cybersanté dans leurs lois ou prévoient de le faire ? Comment le font-ils ?	3.6
Etat de la recherche	Quels avis ont été donnés dans diverses publications sur les questions de droit touchant la cybersanté ?	3.7

3.2 Législation dans un choix de pays

L'équipe de projet a commencé par se faire une idée générale des conditions de base qui existent dans d'autres pays concernant la cybersanté. Il a procédé à une brève recherche sur Internet pour voir si des projets de cybersanté sont prévus ou mis en œuvre dans différents pays et s'il est possible de trouver des réglementations légales à ce sujet. Le groupe s'est limité à des pays qui paraissaient intéressants du point de vue de leur évolution juridique ou technique.

Brève recherche

Dix pays ont finalement été sélectionnés pour une analyse approfondie.

Sélection des pays

Les critères de choix déterminants étaient les suivants : des dispositions légales sur des thèmes de cybersanté sont-elles en préparation ou en vigueur dans le pays en question ? Un engagement dans le domaine de la cybersanté est-il visible ? Des projets sont-ils effectivement réalisés et une documentation à ce sujet est-elle disponible ? Au cours de la recherche approfondie, contact a été pris avec certains des ministères de la santé pour obtenir d'autres informations et faire confirmer les résultats de la recherche.

Allemagne

La loi allemande sur la modernisation de l'assurance-maladie légale (GKV-Modernisierungsgesetz, GMG) oblige les caisses maladie à faire de l'actuelle carte d'assuré une carte de santé électronique. Le § 291a du cinquième code social (SGB V) formule l'obligation d'introduire la carte de santé et en règle les fonctions dans les grandes lignes. Les détails techniques sont définis par l'organisation responsable de la cybersanté Gematik et ont force obligatoire. Les dispositions relatives à la protection des données et à la signature électronique sont inscrites dans les lois correspondantes.

Autriche

En Autriche, un système électronique de gestion (ELSY) a été introduit pour assister les processus administratifs dans le domaine de la santé. Il est envisagé de la combiner avec la carte de citoyen (e-card). Les bases légales d'ELSY, et notamment l'étendue des données administratives et médicales, ont été inscrites dans la loi concernant l'assurance sociale générale (ASVG). La loi sur les services de télésanté règle l'identification, l'authentification (signature électronique) et les droits d'accès des prestataires de soins, ainsi que des aspects de la sécurité des données. La protection des données est réglée par la loi y afférente. L'Autriche est en train de lancer la carte électronique de patient (ELGA). Aucune base légale supplémentaire n'est encore élaborée à ce sujet.

Canada

L'analyse du système canadien montre que l'introduction des technologies de l'information et de la communication dans le domaine de la santé a pu se faire sur la base du cadre légal existant. La question de savoir s'il fallait des règles spécifiques pour la cybersanté s'est posée, et des réponses ponctuelles ont été données. Au Canada, on part du principe que le cybersanté constitue de nouveaux moyens de remplir des tâches déjà définies auparavant. Mais on est conscient que les nouvelles technologies recèlent un potentiel de risque accru. Le souci de protection de la sphère privée de la population concernée (confidentialité des données médicales, droits d'accès et de blocage, aspects de la sécurité des données, etc.) représentent de ce fait un facteur central.

Danemark

Le Danemark dispose d'un portail santé (www.sundhed.dk) accessible en ligne pour les patients et les prestataires de soins. Ses principales applications en ligne sont les suivantes :

- accès aux données de patients des laboratoires et d'autres fournisseurs de prestations ;
- prises de rendez-vous ;
- renouvellement d'ordonnances ;
- consultation par courriel.

Les contacts pris avec le ministère de la Prévoyance sociale n'ont pas permis de trouver des bases légales concernant www.sundhed.dk.

Espagne

L'Espagne a introduit une carte électronique de citoyen et mis en place

un portail de cyberadministration (Servicíos Publicos Digitales). D'après une fiche d'information EER[3], les activités dans le domaine de la cybersanté constituent une partie de la stratégie espagnole de cyberadministration (Plan Avanza). On n'a cependant pas trouvé de chapitre sur la cybersanté dans cette stratégie. Les contacts pris avec le ministère de la Santé n'ont pas permis non plus d'obtenir des informations complémentaires à ce sujet. L'ancrage légal de la protection des données et de la télécommunication date de 1999 et 2003 respectivement, mais les bases légales de la signature électronique, de la télémédecine et des services de santé en ligne ne sont pas encore établies.

Estonie

Les projets estoniens de cybersanté sont réalisés dans le cadre de la législation nationale existante. Outre la législation sur la santé et la loi sur l'information et la protection des données, l'Estonie dispose aussi de lois dans le domaine de la communication électronique. La carte d'identité électronique a été introduite il y a quelques années. Elle a diverses fonctions et est utilisée dans de nombreux domaines. La cyberlégislation règle les questions des technologies de l'information et de la communication (communication électronique, signature électronique, gestion de banques de données, sécurité technique des données, etc.) indépendamment du domaine d'utilisation (cyberadministration, cybercommerce, cybersanté). Les aspects protection et sécurité des données ont gagné en importance. Des règles spécifiques sont intégrées directement dans la cyberlégislation, ou alors on renvoie aux principes formulés dans la loi sur l'information et la protection des données.

France

Les bases légales de la carte d'assuré française (« carte vitale ») sont inscrites dans le Code de la sécurité sociale. La carte vitale sert uniquement à la facturation électronique des prestations médicales et ne contient pas de données médicales. La protection des données est régie par une loi en la matière. Le projet de dossier électronique du patient a été repris en 2008 et se trouve toujours en phase de planification.

Pays-Bas

L'organe néerlandais de coordination de la cybersanté Nictiz, qui a élaboré la stratégie de cybersanté « Aorta », a été fondé en décembre 2001. A partir de 2002, il s'est développé en un partenariat public-privé (PPP). Depuis 2008, il est possible aux Pays-Bas d'obtenir par un guichet national (LSP) des informations tirées d'un dossier de patient enregistré de façon décentralisée. La base légale du *Citizen Service Number* a été adoptée par le Parlement le 10 avril 2008. D'après un rapport EER[4], la législation sur le dossier électronique du patient devait être traitée par le Parlement fin 2007. L'équipe de projet n'a pas obtenu d'informations complémentaires sur ce thème. Elle n'a pas pu trouver non plus de bases légales concernant d'autres thèmes du domaine de la cybersanté.

Slovénie

La Slovénie a introduit avec succès de 1998 à 2000 une carte d'assuré avec des applications administratives et des données d'urgence. La stratégie slovène 2007-2010 en matière de cybersanté prévoit la mise en place du système carte d'assuré (p. ex., accès en ligne via un portail, signature électronique) et l'introduction de nouvelles applications (p. ex., télémédecine et registre électronique des naissances). Malgré des contacts répétés avec le Ministère de la santé, il n'a pas été possible de

[3] eHealth priorities and strategies in European countries, p. 69, disponible à l'adresse : http://www.ehealth-era.org/documents/2007ehealth-era-countries.pdf.

[4] eHealth strategy and implementation activities in the Netherlands, p. 10, disponible à l'adresse : http://www.ehealth-era.org/database/documents/ERA_Reports/eHealth-ERA_Report_Netherlands_03-10-07_final.pdf.

trouver des bases légales concernant la cybersanté en Slovénie.

Le nouveau Patient Data Act, qui constitue la base légale du dossier électronique du patient, est entré en vigueur le 1er juillet 2008. Cette loi prévoit l'introduction d'un dossier patient décentralisé, mais ne règle pas les détails techniques et organisationnels. La nouvelle loi introduit des dérogations à la loi existante sur la protection des données afin de permettre des applications de cybersanté. La Suède a en outre déjà réglé la question de la signature électronique dans la loi sur le cybercommerce.

Suède

L'analyse de la législation relative à la cybersanté dans un choix de pays a mis en évidence qu'aucun pays n'a édicté de loi spécifique. Les règles appliquées, les devoirs professionnels par exemple, sont rédigées en termes neutres du point de vue de la technique. Elles s'appliquent naturellement aussi lorsque les processus d'affaires ou la gestion des dossiers se font, entièrement ou partiellement, par informatique. Là où la question de la communication électronique l'exige, des lois spécifiques ont été édictées, p. ex., les lois sur la signature électronique.

Conclusion

Toutes les prescriptions de la législation sur la protection des données s'appliquent aussi à l'utilisation des technologies de l'information et de la communication. La majorité des pays a inscrit dans la loi des dispositions sévères en matière de protection et de sécurité des données pour le maniement des données sensibles dans le domaine de la télémédecine et du dossier électronique du patient ; des fonctions de surveillance ont parfois été explicitement attribuées aux autorités de protection des données. En Suède, à l'inverse, les règles de protection des données ont plutôt été assouplies pour permettre des applications de cybersanté (p. ex., possibilité d'enregistrer à vie un large éventail de données). En contrepartie, les dispositions relatives à la sécurité des données ont été durcies, et le patient a obtenu un droit d'accès garanti à ses données électroniques en matière de santé.

Dans presque tous les pays qui ont déjà introduit des applications de cybersanté, un organe de coordination de ce domaine a été fondé. Les tâches de ces organes sont diverses, mais elles comprennent presque sans exception l'évaluation et la surveillance du respect des normes techniques déclarées obligatoires sur recommandation des organisations responsables.

Vue d'ensemble de la législation des pays sélectionnés

Annexe 1

3.3 Effets des bases légales sur les activités relevant de la cybersanté dans un choix de pays

Dans le cadre de ses travaux, l'équipe de projet s'est demandé quelles bases légales avaient fait leurs preuves à l'étranger ou avaient au contraire échoué du point de vue des entreprises informatiques. Une brève enquête auprès de sociétés actives sur le plan international a donné les résultats suivants.

Démarche

Le grand désavantage de l'approche descendante (*top down*) allemande est que la carte de santé a été conçue par l'industrie sur le plan technique avant tout. L'implication des personnes concernées a été négligée. La création de la gestion autonome Gematik a été une tentative de remédier à cette lacune. Malheureusement, d'importants groupes d'ayants droit

Allemagne

n'ont pas été pris en compte là non plus. Lorsque la gestion autonome est incapable de prendre une décision du fait de la répartition 50 % / 50 % entre agents financeurs et prestataires de soins, c'est le législateur qui doit décider. Pour cette raison, l'introduction de la carte de santé électronique n'avance que lentement.

Autriche

En Autriche, les applications de cybersanté ont progressé rapidement grâce à l'approche globale adoptée (e-card en tant que carte de citoyen). Dans le domaine de la santé, l'e-card a pu remplacer la feuille de maladie, présentant ainsi une utilité immédiate pour tous les acteurs. Cela a considérablement facilité son acceptation.

Danemark

Au Danemark, ce ne sont pas les bases légales qui ont été la clé du succès de la plateforme de santé. La société anonyme centrale MedCom et le financement par l'Etat à hauteur de 10 millions d'euros par année ont joué un rôle déterminant.

Conclusion

La conclusion générale que l'on peut tirer est que dans tous les pays examinés, l'introduction d'une identité numérique et de standardisations a été la principale base du succès des applications de cybersanté.

3.4 Recoupements avec la cybersanté dans la législation nationale

Recoupements avec la cybersanté

L'équipe de projet a recherché dans la législation fédérale des recoupements avec des thèmes de cybersanté, autrement dit des lois qu'il faudrait adapter le cas échéant dans le cadre de la mise en place d'applications de cybersanté. De tels recoupements se trouvent notamment dans le droit des assurances sociales, de la santé et de la protection des données, dans le code pénal et le code des obligations. L'énumération faite en annexe ne prétend pas à l'exhaustivité. Outre la législation déjà en vigueur, l'équipe de projet a examiné s'il y avait des projets ayant des recoupements possibles avec la cybersanté.

Droit des assurances sociales

Le droit des assurances sociales présente notamment des recoupements avec les thèmes de la carte d'assuré (facturation électronique) et de l'identifiant de personne (numéro d'assuré).

Un éventuel développement de la carte d'assuré administrative en une carte de santé et l'utilisation du numéro d'assuré comme identifiant de patient nécessiteraient la création de bases légales.

Droit de la santé

Des recoupements dans le droit de la santé se trouvent dans la loi sur les professions médicales (registre des professions médicales). La loi sur la prévention en préparation prévoit un portail d'information sur des thèmes de santé. Il faut vérifier si l'introduction de la cyberprescription aurait des effets sur la loi sur les produits thérapeutiques ou la loi sur les stupéfiants.

Droit de la protection des données

La législation sur la protection des données est rédigée en termes neutres du point de vue de la technique. L'emploi des technologies de l'information et de la communication nécessite l'application de cette législation. Un recoupement important pour la cybersanté devrait aussi se trouver dans la possibilité de certifier des organisations et des procédures prévue par la nouvelle ordonnance sur les certifications en matière de protection des données.

Code pénal

L'obligation de garder le secret dans le domaine de la santé (secret médical) est réglée principalement dans le code pénal, qui prévoit des sanc-

tions en cas de violation. Le droit pénal comprend aussi des règles explicites concernant le vol et la détérioration de données électroniques, ainsi que l'abus d'équipements de traitement des données, qui sont également importantes pour la cybersanté.

Code des obligations

Dans le droit privé, l'engagement contractuel régi par le code des obligations implique pour le corps médical des obligations de documentation, de conservation et de communication des documents. Ces règles s'appliquent quels que soient les moyens technologiques utilisés pour produire la documentation. Les obligations de conserver les données médicales sont régies en outre par des dispositions cantonales, qui prévoient, p. ex., des délais de conservation de différentes durées. Le moment à partir duquel ce délai court n'est, la plupart du temps, pas défini.

Autres lois spéciales

Des règles spécifiques pour des domaines particuliers sont fixées dans des lois spéciales (p. ex., loi sur la transplantation, loi fédérale sur l'analyse génétique humaine). Pour le respect de ces règles spécifiques, se pose en pratique le problème de la délimitation de certaines parties du dossier médical.

Autres projets

Il faut examiner si des composantes de l'infrastructure du projet de cyberadministration pourraient être reprises pour la mise en œuvre de la cybersanté. Les projets « Harmonisation des registres » et « Introduction d'un numéro d'identification des entreprises » devraient aussi présenter des synergies.

Conclusion

Les bases légales existantes (p. ex., droits des patients, devoirs professionnels) se trouvent dans de nombreuses lois, et il existe thématiquement de nombreux recoupements avec des applications possibles de la cybersanté, p. ex., la cyberprescription, la facturation électronique des prestations, le dossier électronique du patient, etc. Comme les règles existantes sont formulées en général indépendamment des moyens de traitement et de communication, elles sont également applicables en principe aux utilisations de la cybersanté. Cela vaut en particulier pour la législation sur la protection des données, dont la majeure partie est rédigée en termes neutres du point de vue de la technique et qui prescrit uniquement l'utilisation de mesures techniques et organisationnelles appropriées.

Là où des règles ont déjà été édictées spécialement pour la communication électronique, aucune adaptation ne sera nécessaire. Cela vaut, p. ex., pour la signature électronique, qui est déjà régie par une loi fédérale. Certaines composantes et expériences peuvent également être tirées d'autres projets (cyberadministration, p. ex.).

Annexe 2

Vue d'ensemble des textes de loi et des projets suisses présentant des recoupements possibles avec la cybersanté

3.5 Recoupements avec la cybersanté dans les législations cantonales

Analyse dans les cantons de BS, BE, GE, LU, SG, TI et UR

Même si aucun canton n'a adopté à ce jour d'acte juridique spécifique en matière de cybersanté, il existe dans les législations cantonales en vigueur des dispositions pertinentes qui définissent en plus du droit fédéral le cadre juridique des projets pilotes de cybersanté. Il s'agit en premier lieu des domaines de la protection des données, des droits des patients et des devoirs professionnels des prestataires de soins. Parmi ces de-

voirs figure notamment la tenue d'un dossier médical. Pour le présent chapitre, on a procédé à une analyse de la situation juridique dans les cantons de Bâle-Ville, Berne, Genève, Lucerne, Saint-Gall, Tessin et Uri. Il s'agit des cantons qui se sont déjà montrés actifs dans le domaine de la cybersanté et qui sont donc représentés dans le comité de pilotage de l'organe de coordination cybersanté de la Confédération et des cantons, ainsi que de deux cantons qui n'ont pas encore lancé de projet dans ce domaine, mais qui ont fait part de leur intérêt pour le sujet. Parmi ces derniers, Berne est représentatif des grands cantons et Uri des petits.

Protection des données

La loi fédérale sur la protection des données (LPD) règle le traitement de données concernant des personnes physiques et morales par des personnes privées et des organes fédéraux. Le traitement par des organes cantonaux ou communaux est régi par les lois cantonales (et parfois communales) sur la protection des données. Les lois cantonales contiennent en règle générale des dispositions concernant la collecte, le traitement, l'archivage et la communication de données, le droit de consulter et de rectifier les données ainsi que, parfois, le rôle du préposé cantonal à la protection des données. Les modalités plus précises sont réglées au niveau de l'ordonnance.

Les principes de la protection des données sont repris en outre dans les lois sanitaires cantonales et, dans quelques cantons, dans une loi spéciale ; ils sont, p. ex., confirmés ou renforcés dans les lois sur l'exercice des professions médicales ou les lois sur les droits des patient.

Droits des patients

Les droits des patients résultent de la Constitution fédérale et du code civil. Le principe de la défense des droits des patients est souvent inscrit dans les lois sanitaires cantonales, soit comme chapitre à part, soit comme partie des obligations liées à l'exercice d'une profession du domaine de la santé. On citera à ce titre l'obligation d'information, le droit à l'autodétermination et le droit de consulter son propre dossier médical.

Devoirs professionnels

L'autorisation des membres du corps médical, des autres personnes actives dans des professions de la santé et des praticiens de santé naturopathes à pratiquer leur profession est une tâche cantonale, réglée en général par la législation cantonale en matière de santé. La définition des obligations professionnelles, si elle n'est pas déjà donnée par le droit fédéral (p. ex., LPMéd), est liée à la réglementation de ces autorisations.

Les obligations professionnelles fixées par la loi sur la santé, p. ex., l'obligation de documentation (tenue du dossier médical), résultent déjà du droit du mandat (CO).

Les devoirs professionnels sont, p. ex., l'obligation de prêter assistance, celle d'exercer personnellement la profession, le devoir de diligence, le respect des droits des patients (respect de la dignité humaine du patient, de l'obligation d'information, du droit à l'autodétermination et du droit de consulter son dossier) et l'obligation d'enregistrer. La loi sanitaire cantonale prévoit parfois aussi l'obligation de se perfectionner régulièrement ou celle de conclure une assurance responsabilité civile.

Dossiers médicaux

Une obligation professionnelle importante en lien avec la diffusion du traitement électronique des données est pour les praticiens celle de gérer les enregistrements de leurs notes sur leur activité médicale et sur les patients traités. Dans la plupart des cantons, les médecins et les pharmaciens sont tenus d'établir et de conserver un dossier médical. L'obligation de conservation porte en général sur une durée de dix ans. Les autres

professionnels actifs dans le domaine de la santé peuvent aussi être tenus de conserver les observations enregistrées.

L'obligation de tenir des dossiers médicaux et la définition des contenus sont parfois inscrites dans les lois sanitaires ou hospitalières cantonales, ou dans les ordonnances sur l'exercice de la profession des personnes actives dans le domaine de la santé.

Surveillance

La surveillance du corps médical, des autres professions du domaine de la santé et des hôpitaux est du ressort du département compétent (en général le département de la santé). Partant, les fonctions de surveillance du département, de la commission de surveillance des professions de la santé, du médecin cantonal et des médecins officiels, ainsi que la procédure de recours, sont réglées dans les lois sanitaires cantonales. Les cantons n'ont pas de dispositions en matière de surveillance, de responsabilité ou de mesures disciplinaires qui concernent spécifiquement la cybersanté. Le canton de Genève a élaboré une loi qui prévoit des sanctions administratives en cas de communication non autorisée de données (cf. chap. 3.6).

Télémédecine

Il n'existe pas dans les législations cantonales de base légale explicite pour la fourniture de prestations de télémédecine. Les mêmes dispositions s'appliquent que pour un traitement en contact direct avec la personne. Le canton de Glaris a toutefois précisé dans sa loi sur la santé que l'exercice des professions médicales doit par principe se faire directement sur la personne du patient.

Conclusion

L'enquête montre qu'actuellement, sur le plan législatif, les cantons traitent surtout les thèmes suivants en rapport avec la cybersanté :

- protection des données et droits des patients ;
- obligations professionnelles, y c. tenue de dossiers médicaux.

Il convient d'examiner si et dans quels domaines ces activités législatives devraient être étendues et harmonisées en vue de l'introduction d'un dossier électronique du patient.

3.6 Etat de la législation dans les cantons

Législations cantonales en matière de cybersanté

Comme l'a montré l'enquête du projet partiel « Essais pilotes et PPP », il existe déjà dans quelques cantons des projets pilotes en matière de cybersanté qui ont été lancés avec la participation de l'administration cantonale. Ce chapitre traite des bases légales qui existent dans les cantons pour le domaine de la cybersanté.

Bâle-Ville

Le canton de Bâle-Ville prévoit dans son projet de loi sanitaire cantonale une disposition servant de base légale pour des projets pilotes cantonaux dans le domaine de la cybersanté. Il doit encore élaborer des dispositions d'exécution au niveau de l'ordonnance.

Genève

Le canton de Genève est le seul à avoir créé, avec sa loi sur le réseau communautaire d'informatique médicale (LRCIM), une base légale spécifique pour la cybersanté. Ainsi, l'art. 26 LRCIM règle, p. ex., l'organisation et les détails pour l'utilisation de la carte d'assuré dans des projets pilotes. Le projet de loi a été adopté par le Parlement fin 2008. La loi est entrée en vigueur le 1er avril 2009.

Tessin

Le canton du Tessin a réalisé de 2004 à 2007 un projet pilote en matière

de cybersanté intitulé Rete Sanitaria. Il s'agissait de tester sur une base volontaire une carte d'assuré contenant des données d'urgence. Le projet a été mené à terme et fait l'objet d'une évaluation.

Conclusion

La plupart des cantons n'ont pas encore testé d'application concrète de la cybersanté ou se trouvent encore à cet égard en phase d'élaboration d'un concept. Les projets pilotes lancés jusqu'ici dans les cantons se fondent en gros sur les bases légales existantes. Il n'y a donc pratiquement pas de bases légales cantonales spécifiques pour la cybersanté.

La mise en œuvre à l'échelle nationale d'essais pilotes utilisant la carte d'assuré nécessiterait la création de bases légales correspondantes au niveau des cantons. L'enquête a cependant montré qu'il n'existe pour l'heure quasiment aucun projet de loi, même en préparation.

Vue d'ensemble de l'état de la législation dans les cantons — Annexe 3

3.7 Etat de la recherche

Remarque générale

La littérature sur les bases légales dans le domaine de la cybersanté a trait surtout à l'introduction d'une carte de santé et aux aspects de protection et de sécurité des données. Les PPP dans le domaine de la santé et les bases légales pour la télémédecine et le dossier électronique du patient sont, en revanche, peu étudiés.

Protection des données

Dans le domaine de la protection des données, on met régulièrement en lumière le rapport conflictuel entre le progrès technique et la protection des données des patients. De nombreux auteurs traitent des exigences en matière de protection des données posées aux applications de cybersanté, exigences qu'ils définissent comme facteur de sécurité et condition de succès pour l'ensemble du système.

Répartition des compétences défavorable pour la cybersanté

On trouve dans la littérature la thèse selon laquelle la répartition des compétences entre la Confédération et les cantons dans le domaine de la santé ne serait pas clairement réglée, ce qui serait particulièrement défavorable pour le domaine de la cybersanté (processus d'ensemble).

Etranger

Quelques travaux commentent la législation d'un choix de pays en matière de cybersanté ou les directives de l'Union européenne sur ce thème.

Vue d'ensemble de l'état de la recherche — Annexe 4

3.8 Bilan

Les bases légales ne sont pas un facteur clé pour faire avancer la cybersanté

Tant au plan international que national, il y a peu d'éléments à disposition qui permettraient de reprendre directement des solutions dans le domaine des bases légales. Tout semble indiquer plutôt que chaque pays trouve sa propre solution, c.-à-d. que les bases sont adaptées au système juridique particulier. Cela invite à conclure que les bases légales ne constituent pas le facteur déterminant s'agissant de faire avancer la cybersanté avec succès.

Conclusions

Au terme de l'analyse de la situation, il est possible de tirer les conclusions suivantes :

- Pas de loi spécifique pour la cybersanté : les réglementations

existantes sont formulées en général indépendamment des moyens de traitement et de communication employés. Elles s'appliqueront toutes naturellement aussi lorsque, à l'avenir, les processus des affaires ou la gestion des dossiers se feront, entièrement ou partiellement, par l'informatique. Là où la question de la communication électronique l'exige, il faudra édicter des dispositions visant spécifiquement la cybersanté.

- La protection des données est d'une importance capitale : l'analyse de la situation a montré que la protection de la personnalité des intéressés joue un rôle primordial lorsque l'on a recours aux technologies de l'information et de la communication. Il devrait donc être indiqué de définir plus concrètement dans une future législation concernant la cybersanté les exigences en matière de protection des données, du moins pour certaines applications (p. ex., dossier électronique du patient, cyberprescription).
- Identification et authentification des acteurs du système : l'identification et l'authentification sans ambiguïté des patients et des fournisseurs de prestations sont des conditions indispensables aux applications de la cybersanté (p. ex., dossier électronique du patient, cyberprescription).

4 Besoin d'adaptations légales

4.1 Démarche

Démarche : diviser le travail en une série de « paquets »

Les champs thématiques suivants ont été sélectionnés et étudiés pour se faire une idée du besoin d'intervention dans le domaine du droit :

Thème	Question	Chapitre
Responsabilité de l'organe de coordination de la cybersanté	Jusqu'où la responsabilité de l'organe de coordination de la cybersanté doit-elle être inscrite dans le droit ?	4.2
Dossier électronique du patient	Quels thèmes faut-il régler pour le dossier électronique du patient ?	4.3
Protection et sécurité des données	A quel point les principes de protection des données doivent-ils être concrétisés pour le domaine de la cybersanté ?	4.4
Droits et obligations	Quels groupes d'acteurs ont quels droits et quelles obligations ?	4.5
Identification, authentification et autorisation	Quels éléments d'identification, d'authentification et d'autorisation sont nécessaires et doivent être inscrits dans la loi ?	4.6
Autres thèmes (responsabilité, surveillance, financement, sanctions et mesures, etc.)	Quels autres instruments doivent être inscrits dans la loi pour que le système fonctionne ?	4.7

Besoin d'intervention décelé par les cinq autres projets partiels

En vue de coordonner les activités des différents projets partiels, le secrétariat leur a donné l'occasion de se poser des questions les uns aux autres. En outre, la Société suisse de télémédecine et eHealth a formulé des questions juridiques du point de vue des fournisseurs de prestations de télémédecine. Ces questions font l'objet des travaux ci-après.

4.2 Responsabilité de l'organe de coordination de la cybersanté

Situation de départ : tous les pays créent une organisation responsable

L'analyse de la situation a montré que la plupart des pays qui ont des activités de cybersanté ont créé un organe de coordination de ce domaine. La création d'un tel organe semble indiquée en Suisse aussi. A cet égard, les points énumérés ci-dessous doivent être inscrits dans le droit. Une analyse de la forme juridique appropriée sera faite dans le cadre de la formation des variantes. La décision à ce propos sera prise dans une phase ultérieure du projet.

Contenu des dispositions	Thèmes à régler
Principe, fondateur Détermination du support juridique de l'organe de coordination de la cybersanté (exemple : l'art. 18, al. 1, LAMal définit le responsable chargé de créer l'institution commune LAMal).	
Forme juridique Définition de la forme juridique (exemple : l'art. 18, al. 1, LAMal définit que la forme juridique de l'institution commune LAMal est la fondation).	
Exécution par substitution Réglementation éventuelle pour le cas où les acteurs ne peuvent se mettre d'accord sur la création de l'organe de coordination (exemple : art. 18, al. 1, LAMal).	
Tâches et compétences Liste des tâches et des compétences de l'organe de coordination (exemple : art. 18, al. 2 à 2^{sexies}, LAMal).	
Organisation Règles sur l'organisation du support juridique (exemple : art. 18, al. 3, 4 et 7, LAMal).	
Financement Règles sur le financement de l'organe de coordination (exemple : art. 18, al. 5 et 5^{bis}, LAMal).	
Voie de recours Règles sur la procédure de recours (exemple : art. 18, al. 8, LAMal).	

Un besoin d'intervention existe. — Conclusion

4.3 Dossier électronique du patient

Le but visé par l'ancrage légal du dossier électronique du patient est de créer une base juridique favorisant le succès de la mise en œuvre de la cybersanté. Par dossier électronique du patient, on n'entend pas l'ensemble de la documentation relative au patient (dossier médical) chez chaque prestataire de soins, mais une partie de celle-ci, à définir, qui comprend des documents importants pour la suite du traitement. Seule cette partie doit être consultable électroniquement par d'autres prestataires de soins autorisés. Pour cela, il s'agit de prescrire aussi peu que possible, mais de régler autant que nécessaire. Les bases légales doivent se focaliser sur les personnes concernées (patients, utilisateurs), mais aussi permettre au système de continuer à se développer techniquement. Il faut pour cela que les dispositions soient formulées de manière très ouverte.

Philosophie de base : une réglementation ouverte

Le chemin menant au dossier électronique du patient préparera aussi le terrain pour d'autres applications de la cybersanté. C'est pourquoi l'accent est mis d'abord sur ledit dossier électronique du patient. Les bases légales en définiront les principaux éléments, sans fermer la porte à

Le dossier électronique du patient, application clé

d'autres applications.

Contenu du dossier électronique du patient

L'introduction du dossier électronique du patient se concentre dans une première phase, suivant les recommandations du projet partiel « Normes et architecture », sur le domaine des processus cliniques entre prestataires de soins, deux de ces processus étant considérés comme prioritaires :

- échange d'informations le long de la chaîne de traitement ;
- prescription intégrée de médicaments.

Ils sont à comprendre comme les premiers pas sur la voie de l'introduction du dossier électronique du patient et ne signifient pas, à ce stade, la tenue d'un dossier médical informatisé.

Thèmes à régler

Contenu des dispositions
Principe, destinataire Introduction du dossier électronique du patient avec description des responsabilités relativement à l'établissement et à la gestion du dossier (ex. : art. 1, al. 1, OCA).
But Définition du but du dossier électronique du patient (traitement) (ex. : art. 42*a*, al. 2, LAMal), y c. buts accessoires éventuels (recherche, expertises, etc.). Règles relatives au maniement des données des patients pour des buts accessoires tels que la recherche ou la statistique (pilotage du système de la santé) avec principe de l'anonymat, obligation de recueillir le consentement du patient, etc.
Procédure et organisation Règles relatives au fonctionnement du dossier électronique du patient (ex. : art. 15, al. 4, OCA).
Catégories de données Etendue des données qui peuvent ou doivent être utilisées en relation avec le dossier électronique du patient (ex. : art. 1, al. 1, OCA). L'étendue nécessaire doit être définie en collaboration avec les prestataires de soins.
Protection et sécurité des données Voir ch. 4.4.
Délégation Délégation des règles concernant les normes techniques et les détails organisationnels au niveau de l'ordonnance (ex. : art. 17 OCA).

Adaptation des dispositions sur la carte d'assuré

Il est probable que le développement d'applications de cybersanté déjà introduites par l'ordonnance sur la carte d'assuré (OCA) (procédure en ligne, p. ex.) se poursuivra dans le cadre du projet Cybersanté. Il faut donc examiner s'il y a lieu d'adapter les dispositions correspondantes de l'OCA. On ne sait pas encore si ces dispositions resteront dans l'OCA ou s'il faudra les abroger et les transférer dans un autre texte de loi. Au cas où la carte d'assuré serait perfectionnée pour servir de clé d'accès au

dossier électronique du patient, il faudrait inscrire dans la loi la séparation des fonctions carte d'assuré (purement administrative) et carte de santé (accès à des informations médicales).

Un besoin d'intervention existe.

Conclusion

4.4 Protection et sécurité des données

En Suisse, la protection et la sécurité des données sont réglées dans la loi fédérale et les lois cantonales sur la protection des données. Les dispositions de ces lois sont formulées de façon générale et abstraite. Elles devront être concrétisées et, le cas échéant, adaptées pour le domaine de la cybersanté. Il sera justifié de les rendre plus sévères sur certains points (p. ex., le maniement de données sensibles relatives aux patients) ou d'adapter suivant les cas les lois spéciales, afin de ne pas empêcher d'emblée certaines utilisations.

Principe : concrétisation de la réglementation en matière de protection des données

Contenu des dispositions	Thèmes à régler
Proportionnalité Pour le dossier électronique du patient, il faut créer la possibilité d'enregistrer électroniquement pour une longue durée une partie au moins des données relatives à la santé des patients, afin qu'il soit possible d'y accéder. Cela peut être en contradiction avec le principe de proportionnalité fixé à l'art. 4 LPD (quantité maximale et non minimale de données ; durée de conservation aussi longue et non pas aussi courte que possible, etc.). En contrepartie, la proportionnalité peut être prescrite plus strictement sur d'autres points (accès différencié ; prescriptions d'anonymisation et de cryptage, etc.).	
Adéquation Définition du but de chaque application de cybersanté (le cas échéant, distinction entre buts principaux et buts accessoires d'où, au besoin, des conditions différentes pour les différents buts ou pour un changement de but). L'affectation à un but défini implique que les données ne peuvent être traitées que pour le but qui a été indiqué au moment de l'acquisition des données, qui est prescrit par la loi ou qui ressort du contexte. Pour cela, le but du traitement doit être décrit exactement par le détenteur du fichier et être connu des acteurs. Un changement ultérieur du but, p. ex., l'élargissement du groupe des institutions autorisées à accéder aux données, doit également respecter les dispositions légales ou les accords conclus.	
Transparence Principe de la transparence lors du traitement électronique de données.	
Définition des termes employés Définition de termes nécessaires (termes nouveaux ou plurivoques, termes techniques, applications de cybersanté, etc.).	
Catégories de données (cf. ch. 4.3) Les données nécessaires devront être définies par les prestataires de soins. Le modèle classique des listes exhaustives de données n'est plus guère applicable dans le contexte de la cybersanté. On peut prévoir à la place des degrés de protection différents pour des groupes de données différents, ainsi que des conditions pour le maniement de telles données.	
Groupes de données avec différents niveaux de protection Vu son contexte, le domaine de la cybersanté a toujours affaire à des données sensibles au sens de la loi sur la protection des données. Mais la sensibilité de certains groupes de données peut être plus ou moins grande. Il est possible d'en tenir compte en distinguant des groupes selon le degré de protection nécessaire, p. ex. : ➢ données identifiantes ; ➢ données administratives ; ➢ données médicales générales (pas particulièrement sensibles) ; données médicales spéciales (particulièrement sensibles).	

Information des patients Information active complète, cf. ch. 4.5.
Autorisation du patient Nécessité et forme de l'autorisation du patient, manière de procéder pour obtenir une autorisation ainsi que la documentation.
Droits d'accès et communication de données Droits d'accès des prestataires de soins en fonction de leur rôle (usage interne, cf. ch. 4.6), réglementation de communication éventuelle des données à des tiers (externes), modalités de la communication, restrictions particulières pour la transmission de données médicales particulièrement sensibles.
Externalisation Possibilité et conditions d'externalisation du traitement de données.
Sécurité des données Définition plus précise des mesures de sécurité des données (art. 7 LPD) : exigences plus élevées requises pour les mesures techniques et organisationnelles ou mesures techniques supplémentaires de protection pour certaines applications en raison de la complexité du traitement électronique des données et du plus grand potentiel de risque qui en résulte. Il faut garantir de la même manière la confidentialité, la disponibilité, l'intégrité et l'authenticité des données.
Journalisation des accès Obligation de journaliser les accès aux données des patients. Un document doit indiquer de manière compréhensible qui a traité quelles données, quand et de quelle façon : définition du contenu et délai de conservation du fichier-journal.
Mécanismes de protection particuliers Recours aux techniques de sécurisation des données : ➢ mesures techniques de protection particulières pour les données au degré de protection élevé ➢ instruments de création de pseudonymes et d'anonymisation (définition des exigences minimales en matière d'anonymisation) ➢ principe de séparation des données : séparer les données identifiantes des autres (p. ex., dans le dossier du patient) ➢ cryptage (pour l'enregistrement et la transmission de données) ➢ signature électronique ➢ autres (suivant l'application)
Archivage des données Prescriptions d'archivage (p. ex., accès au dossier du patient rendu plus difficile après l'achèvement du traitement).

Elimination des données Prescriptions d'élimination (pour les dossiers, les données électroniques, les moyens informatiques, etc.).
Autorité de surveillance : cf. ch. 4.7.

Conclusion

Un besoin d'intervention existe.

4.5 Droits et obligations

Droits *(P : patient, S : prestataires de soins, A : assureurs)*	**P**	**S**	**A**
Caractère facultatif Caractère facultatif du système (la non-participation ne doit pas entraîner de désavantage, principe du non-exercice d'une influence).	x	(x)	
Droit d'être informé sur le traitement des données Information sur le lieu et la manière dont les données sont enregistrées dans le système et sur la personne habilitée à consulter et traiter ces données ou à qui elles peuvent être communiquées, à quelles fins et dans quelles conditions. Information sur les mesures de sécurité des données et sur la possibilité de les bloquer. Information du patient sur ses droits, notamment d'être renseigné, de rectifier ou de bloquer les données.	x		
Droit d'être renseigné Droit usuel d'obtention de copies conformément à la LPD ; à compléter par le droit d'être renseigné sur l'origine des données et le droit d'accès aux données du fichier-journal.	x		
Droit d'accès direct à son propre dossier électronique de patient Droit d'obtenir une clé d'accès (p. ex., carte d'assuré à usage étendu) et information sur la manière d'accéder aux données/documents et aux possibilités ou restrictions qui y sont liées (p. ex., droit de faire mention d'un désaccord, mais non d'effacer des données, etc.).	x		
Droit de rectifier des données Droit de rectifier des données objectivement fausses.	x	(x)	
Droit de bloquer des données Droit de bloquer des informations hautement personnelles ou litigieuses.	x		
Droit à l'anonymat Droit à l'anonymat ou à l'usage d'un pseudonyme lors de la transmission de ses propres données à des tiers (introduction du principe de l'anonymisation).	x		
Droit d'effacer des données Droit de supprimer des documents du dossier électronique du patient ; non d'en effacer le contenu, mais le cas échéant de mentionner un désaccord (cf. ci-dessus « Droit d'accès »).	x	(x)	

Droits

Obligations

Obligations *(P : patient, S : prestataires de soins, A : assureurs)*	**P**	**S**	**A**
Obligation d'informer le patient Obligation d'informer le patient sur le traitement des données (sur le lieu et la manière dont les données sont enregistrées dans le système et sur qui peut consulter et traiter ces données ou à qui elles peuvent être communiquées, à quelles fins et dans quelles conditions. Information sur les mesures de sécurité des données et sur la possibilité de bloquer les données) – ex. : art. 9 à 13 OCA.		x	x
Obligation de facturation électronique Obligation éventuelle de procéder à la facturation électronique conformément à l'art. 42*a* LAMal, y c. droits et obligations réglés dans l'OCA.	(x)	x	
Obligation de formation Obligation de former le personnel qui traite les données (applications informatiques, protection des données).		x	x
Obligation de tenir le dossier électronique du patient En cas de participation au système, obligation de tenir le dossier électronique du patient.		x	
Obligation d'archivage Obligation d'archivage, éventuellement avec accès rendu plus difficile aux données archivées, réglementation de la durée d'archivage dans le dossier électronique du patient.		x	

Conclusion

Un besoin d'intervention existe.

4.6 Identification, authentification et autorisation

Identification, authentification et autorisation des différents acteurs

La sécurité dans l'identification et l'authentification des différents acteurs, ainsi que leur autorisation à consulter ou traiter les données des patients, sont d'une extrême importance. Selon toute vraisemblance, la définition de règles claires en la matière favorisera considérablement l'acceptation de l'ensemble du système par tous les participants.

Identification

Les règles relatives à l'identification des participants au système comprennent les éléments de l'identité numérique, les exigences de qualité auxquelles doit satisfaire cette identité, le service qui délivre les certificats et les modalités du processus d'enregistrement.

Authentification

Pour l'authentification, il importe de définir la nécessité de l'authentification, la technique d'authentification, le service qui délivre les certificats et les modalités du processus d'enregistrement.

Autorisation

Les dispositions relatives à l'autorisation porteront sur les droits d'accès des différents participants au système en fonction de leur rôle, l'étendue du traitement des données, l'historique des accès et les droits de repré-

sentation. Il faut également prévoir le droit des fournisseurs de prestations d'accéder aux données en cas d'urgence.

Un besoin d'intervention existe. Conclusion

4.7 Autres thèmes

Différents autres thèmes doivent être tirés au clair et réglés le cas échéant en vue de la mise en œuvre de la cybersanté. Différents autres thèmes à régler

Responsabilité Responsabilité

Les mêmes règles s'appliquent aux documents électroniques qu'aux documents papier. La responsabilité (p. ex., du contenu du document électronique) doit être la même que pour l'établissement d'un document papier usuel. La différence est que le document électronique doit être protégé contre les manipulations ultérieures, car une modification après coup n'est pas toujours constatable. Il doit donc être possible de voir qui, à quel moment, a établi, déposé ou modifié le document. Il faut le cas échéant que la possibilité même de modifier un document déposé dans le dossier électronique du patient soit techniquement exclue. La garantie des exigences supplémentaires est obtenue par le recours à des instruments de sécurité spécifiques (signature électronique, journalisation, etc.). L'usage d'une technique spéciale ne change rien à la responsabilité « habituelle » du médecin.

Concernant la responsabilité des différents acteurs du système :

- Prestataire de soins : celui qui établit le document assume la responsabilité de son exactitude au moment où il est établi. Il doit être protégé contre les manipulations. Rien ne doit être changé à la responsabilité de l'auteur du document par rapport à l'établissement d'un document papier.
- Fournisseur d'accès : assume la responsabilité de la prestation de service technique. Les règles habituelles s'appliquent : responsabilité contractuelle et extracontractuelle (CO), responsabilité pénale (CP), responsabilité prévue par des lois spéciales, p. ex., responsabilité du fait des produits.
- Administrateur du dossier électronique du patient : si cette fonction devait s'avérer nécessaire, les obligations de celui qui l'exerce (p. ex., le médecin de famille) devraient être réglées (p. ex., retirer du dossier les documents dépassés). La question ne se prose probablement qu'en cas d'archivage centralisé. Si cette tâche devient une nouvelle tâche médicale, elle devrait être couverte par la responsabilité civile professionnelle habituelle.
- Fournisseur de services de certification et organisme de reconnaissance (signature électronique) : réglé à l'art. 16 de la loi sur la signature électronique.
- Détenteur de la clé de signature : réglé à l'art. 59*a* du code des obligations.

Dans l'état actuel des informations sur l'ensemble du système, il n'y a donc pas de besoin d'intervention dans le domaine de la responsabilité. Reste éventuellement à examiner le cas de la télémédecine, discipline

« transversale » (cf. ch. 4.8).

Surveillance — Surveillance

- La surveillance de l'exécution de l'assurance-maladie sociale est, conformément à l'art. 21, al. 1, LAMal en corrélation avec l'art. 24, al. 1, OAMal, du ressort de l'OFSP. Il n'est pas nécessaire de modifier ces dispositions pour le domaine de la cybersanté. Il n'y a pas de besoin d'intervention ici.
- Détermination de la surveillance exercée sur :
  - les applications de cybersanté (p. ex., dossier électronique du patient, portail sur la santé, …) ;
  - l'organe de coordination de la cybersanté ;
  - la sécurité des éléments et applications informatiques ;
  - les aspects éthiques liés à la recherche, aux expertises médicales et à d'autres changements de but éventuels.

Financement — Financement

- Dispositions sur le financement de l'organe de coordination
- Dispositions sur le financement et la compétence des composantes de l'architecture
- Dispositions sur le financement des applications de cybersanté (financement initial)
- Réglementation du remboursement des prestations de service supplémentaire apportées par les fournisseurs de prestations dans le domaine de la cybersanté (prestation LAMal ou non).

Mesures d'incitation — Mesures d'incitation

- Incitations (financières) pour encourager un certain comportement.

Certification — Certification

- Prévoir éventuellement des incitations à la certification, p. ex., des privilèges comme l'utilisation facilitée des données pour un but modifié (p. ex., possibilités d'exploitation des données en cas d'usage de techniques de sécurité particulières).

Sanctions et mesures — Sanctions et mesures

- La plupart des sanctions et mesures sont réglées dans les lois sur la protection des données et dans le CP, et applicables au domaine de la cybersanté. Examiner si la négligence peut aussi, comme l'intention, avoir pour conséquence des sanctions et des mesures.
- Prévoir en outre des dispositions rendant punissable l'accès non autorisé à des données personnelles.

Dispositions transitoires — Dispositions transitoires

- Fixer la date d'introduction des diverses applications (éventuellement introduction échelonnée).

Un besoin d'intervention existe. — Conclusion

4.8 Thèmes soulevés par les autres projets partiels

Questions posées par les autres projets partiels

Les questions posées au projet partiel « Bases légales » par les autres projets partiels montrent que sur certains points, on ne sait pas encore clairement quel projet partiel est responsable du contenu. Les questions suivantes ont été posées :

Projet partiel « Normes et architecture »

Projet partiel « Normes et architecture »

Questions	Réponses
Qui est responsable des copies et des extraits du dossier du patient ?	La répartition des rôles dans le système doit être réglée dans le cadre du projet partiel « Normes et architecture ».
Doivent-ils aussi être effacés lorsque les originaux le sont ?	Des règles d'archivage spéciales doivent être créées pour le dossier électronique du patient (ex. : conservation à vie). Il est possible que les originaux soient effacés et que les copies restent dans le dossier électronique du patient.
Les documents doivent-ils être effacés à l'expiration du délai de conservation ?	Voir ci-dessus
Délais de conservation différents : sont-ils valables pour chaque documentation ou pour l'ensemble de la documentation ?	Voir ci-dessus
A partir de quel événement court le délai de conservation ?	Voir ci-dessus

Projet partiel « Essais pilotes et PPP »

Projet partiel « Essais pilotes et PPP »

Question	Réponse
Examiner le texte type du canton de Bâle-Ville et le compléter ou le modifier le cas échéant.	Un nouveau texte type a été rédigé.

Projet partiel « Services en ligne et culture sanitaire »

Projet partiel « Services en ligne et culture sanitaire »

Questions	Réponses
Quelles sont les bases juridiques pour parler de la protection des données des patients ?	Cf. rapport intermédiaire du PP « Bases légales », analyse de la situation, ch. 2.4 (législation nationale) et 2.5 (législations cantonales), pp. 10 à 13.
Comment peut-on informer la population sur ce thème (culture sanitaire) ?	Cela doit être inscrit dans les droits et obligations de chaque groupe d'acteurs.
Quelles sont les bases légales pour l'élaboration d'un portail de	Art. 9 de l'avant-projet de loi sur la prévention (LPrév).

cybersanté ?	
Quelles sont les bases légales concernant le dossier patient ?	Actuellement, la documentation des prestataires de soins est réglée dans les lois cantonales, cf. chap. 3. De nouvelles bases légales doivent être créées pour le dossier électronique du patient.
Sur quoi se baser pour régler la question de responsabilité concernant : - un label national de qualité de l'information en ligne ; - un portail eHealth ; - des services en ligne eHealth ; - la gestion et protection des données personnelles (VeKa + dossier électronique du patient) ?	Les bases légales seront créées en fonction de la solution concrète adoptée.
Que le PP « Bases légales » présente les bases juridiques/ légales existantes de manière simplifiée afin de pouvoir en tirer des informations utilisables pour la population (culture sanitaire).	Cf. rapport intermédiaire du PP « Bases légales », analyse de la situation, ch. 2.4 (législation nationale) et 2.5 (législations cantonales), pp. 10 à 13.

Projet partiel « Formation »

Projet partiel « Formation »

Question	Réponse
Existe-t-il une documentation sur les réflexions qui contienne les décisions liées à la protection des données et aux normes en matière de cybersanté ? Les motifs pour lesquels les règles ont été fixées et de quelle façon doivent être clairs pour la formation.	Sera intégré dans le commentaire les nouvelles règles en matière de protection des données. Concernant la LPD/OLPD : cf. message sur la loi, commentaire de l'ordonnance, travaux préparatoires de la révision de la LPD, etc. (à consulter, p. ex., sur le site www.edoeb.admin.ch).

Les questions seront intégrées dans les travaux de suivi.

Conclusion

4.9 Bilan

Bilan

Il existe un besoin d'intervention au niveau des bases légales dans tous les domaines thématiques étudiés. Les points en suspens concernent surtout des questions qui résultent directement de l'utilisation des nouvelles technologies de l'information et de la communication (p. ex., nécessité d'une identité numérique). Des informations sur l'organisation du système seront nécessaires en temps utile pour préciser davantage les bases légales.

- Pour définir les contenus, il faut attendre les résultats du PP

« Normes et architecture ».

- Des examens seront entrepris dans l’intervalle sur des thèmes qui sont indépendants de l’organisation du système.

5 Recherche de solutions

5.1 Procédure suivie

Formation de « paquets de travail »

Le projet partiel « Normes et architecture » a présenté fin octobre 2008 ses recommandations ainsi qu'un rapport explicatif. Les autres activités du projet partiel « Bases légales » ont été planifiées sur la base de ces travaux et divisées en « paquets de travail » comme suit :

PT	Thème	Questions
1	Répartition des compétences entre Confédération et cantons et coordination au sein de l'Etat	- Clarification de la répartition des compétences entre Confédération et cantons pour la création de bases légales relatives au dossier électronique du patient ; - coordination possible entre la Confédération et les cantons, d'une part, et entre les cantons, de l'autre.
2	Responsabilité de l'organe de coordination de la cybersanté	Réponse aux questions suivantes pour l'ensemble des thèmes à régler (cf. tableaux Besoin d'intervention, chap. 4) : - La compétence de réglementer appartient-elle à la Confédération ou aux cantons ? Des variantes sont-elles imaginables ? Quelle serait la solution la plus utile ? Quelles mesures devraient être prises pour cela ? - Dans quelles lois ces points devraient-ils être inscrits ? Y a-t-il des variantes ? - A quel niveau ce thème doit-il être réglé (loi ou ordonnance) ?
3	Dossier électronique du patient et autres applications	
4	Protection et sécurité des données	
5	Droits et obligations	
6	Identification, authentification et autorisation	
7	Autres thèmes (responsabilité civile, surveillance, financement, sanctions et mesures, règles de procédure)	

Primo : concentration sur la répartition des compétences et la coordination au sein de l'Etat

Il est vite apparu clairement que le traitement des paquets 2 à 7 dépendait de la réponse apportée au paquet 1. Il a donc été décidé de reporter ces travaux et de se concentrer sur ces deux questions principales :

- répartition des compétences entre Confédération et cantons pour la mise en œuvre de la stratégie suisse de cybersanté (ch. 5.2) ;
- formes de coordination nationale dans le domaine de la mise en œuvre de la stratégie suisse de cybersanté (ch. 5.3).

Secundo : inscription des contenus dans le droit fédéral

Diverses possibilités d'inscription dans le droit fédéral (du dossier électronique du patient en particulier) ont en outre été élaborées (ch. 5.4) et l'on a examiné qui pourrait assumer à l'avenir la responsabilité de l'organe de coordination (ch. 5.5). Des résultats intermédiaires sont disponibles pour

le paquet 6 « Identification, authentification et autorisation » (ch. 5.6). Les autres thèmes seront abordés dans les travaux de suivi.

Les recommandations formulées sont des décisions prises à la majorité par le projet partiel « Bases légales » et, pour certaines, par le comité de pilotage (séance du 22 janvier 2009).

Les recommandations sont des décisions prises à la majorité

5.2 Répartition des compétences entre la Confédération et les cantons

La Confédération dispose de plusieurs compétences plus ou moins limitées pour favoriser l'utilisation de l'infrastructure informatique dans l'esprit de la stratégie en matière de cybersanté. Les articles de la Constitution fédérale qui présentent un intérêt en relation avec la cybersanté sont surtout les suivants (par ordre thématique).

Compétence fédérale limitée

Nature de la compétence fédérale	**Article**
Compétence générale dans le domaine de l'assurance-maladie et de l'assurance-accidents (en particulier mesures visant la sécurité du traitement, la qualité et l'économicité).	117 Cst.
Compétence limitée dans le domaine de la protection de la santé (mesures de lutte contre les maladies transmissibles, les maladies très répandues et les maladies particulièrement dangereuses).	118 Cst.
Compétence de réglementer la procréation médicalement assistée et le génie génétique dans le domaine humain.	119 Cst.
Compétence de réglementer la médecine de la transplantation.	119*a* Cst.
Compétence de légiférer sur l'exercice des activités économiques lucratives privées (p. ex., LPMéd).	95 Cst.
Compétence générale dans le domaine du droit civil fédéral (notamment droit du mandat).	122 Cst.

La tenue d'un dossier électronique circonstancié du patient, telle que la vise la stratégie en matière de cybersanté, ne peut se fonder de manière générale sur les dispositions constitutionnelles relatives à la santé. La Confédération peut réglementer de manière exhaustive, sur la base de l'art. 117 Cst., le domaine de l'assurance-maladie et de l'assurance-accidents. La nature du dossier électronique du patient concerne cependant le rapport entre prestataires de soins et patient, qui va plus loin que l'aspect du droit des assurances sociales. La compétence qu'elle a dans le domaine de la protection de la santé (art. 118 Cst.) habilite certes la Confédération à légiférer de manière exhaustive et définitive, mais uniquement dans le secteur limité de la lutte contre les maladies transmissibles, les maladies très répandues et les maladies particulièrement dangereuses. Les compétences dans le domaine de la réglementation de la procréation médicalement assistée et du génie génétique (art. 119 Cst.) ainsi que de la médecine de la transplantation (art. 119*a* Cst.) n'autorisent non plus la Confédération à prescrire des obligations de documentation que pour ces domaines partiels. Or le dossier électronique du patient sert d'abord à la fourniture des soins, qui est du ressort des

cantons. La Confédération ne dispose d'aucune compétence dans ce domaine.

Fonder la tenue du dossier électronique du patient sur les compétences de la Confédération dans le domaine du droit privé (art. 95 et 122 Cst.) ferait également apparaître une lacune. En particulier, les membres du corps médical travaillant dans le secteur public, donc, p. ex., les employés des hôpitaux (cantonaux) de droit public, ne seraient pas inclus, car ce secteur est de la compétence des cantons.

Vu la manière dont la situation se présente pour ce qui est des compétences, trois manières de procéder (variantes) sont proposées pour la mise en œuvre de la stratégie en matière de cybersanté.

Variante 1 : création d'une compétence fédérale en modifiant la Constitution fédérale

Modification de la Cst.

La compétence de légiférer pour régler les principes dans le domaine de la couverture sanitaire est accordée à la Confédération par une modification de la Constitution.

Conclusion :

Cette variante recèle un risque difficile à évaluer (processus politique de formation d'une opinion, déplacement de compétences cantonales au niveau fédéral) et entraîne un retard considérable. Une compétence fédérale dans le domaine de la couverture sanitaire ne paraît pas indispensable pour atteindre l'objectif prioritaire, qui est l'utilisation des techniques modernes dans le domaine de la santé. D'après les résultats de l'audition de mai-juin 2009, la question de savoir si une modification de la Constitution est nécessaire doit recevoir une réponse définitive dans le cadre du processus législatif.

Variante 2 : utilisation maximale des compétences fédérales existantes

Utilisation maximale des compétences fédérales

La stratégie nationale en matière de cybersanté est appliquée au moyen d'une interprétation extensive des compétences fédérales existantes, notamment celles dans le domaine de l'assurance-maladie et accidents (points de référence possibles : qualité et économicité, art. 56 et 58 LAMal, éventuellement règles de la LPGA ; voir explications au ch. 5.4) et de la protection de la santé (p. ex., le portail d'information dans la future loi sur la prévention), ainsi que celle de réglementer l'exercice d'une activité lucrative dans l'économie privée (art. 40 LPMéd, devoirs professionnels). La Confédération réglemente tout ce qui est possible, du point de vue juridique et politique, dans le cadre de ses compétences.

Conclusions :

- Cette manière de faire est problématique du point de vue constitutionnel, car les compétences fédérales existantes sont trop lacunaires pour réglementer entièrement cette matière.
- Il serait possible d'édicter de cette manière des dispositions de droit fédéral allant aussi loin que possible, notamment concernant le dossier électronique du patient ; des lacunes apparaîtraient cependant au niveau de l'application des lois fédérales en raison de compétences fédérales trop étroites, voire absentes.
- Les lacunes dans la réglementation et les règles relevant exclusivement de la compétence des cantons devraient être comblées ou édictées dans le droit cantonal.

Variante 3 : réglementation par la Confédération et les cantons dans leurs domaines de compétences respectifs

Confédération et cantons règlent ce qui relève de leur compétence

La Confédération et les cantons réglementent ce qui relève de leurs domaines de compétences respectifs. La coordination entre les cantons est laissée à l'appréciation de ces derniers (cf. ch. 5.3).

Conclusions :

- La coordination matériellement nécessaire dans l'édiction et la mise en œuvre des réglementations cantonales nécessite une volonté des cantons dans ce domaine.
- On ne sait pas dans quelle mesure les cantons sont prêts à coordonner la mise en œuvre des réglementations relevant de leur compétence au moyen d'un concordat ou autrement.

Le comité de pilotage, à sa séance du 22 janvier 2009, a recommandé de mettre en œuvre la stratégie en recourant le plus possible aux compétences sur le plan fédéral, et en comblant les lacunes restantes par une coordination cantonale. Le droit fédéral offre plusieurs points de référence possibles pour l'ancrage légal du principe du dossier électronique du patient (cf. ch. 5.4.).

Recommandation du comité de pilotage du 22 janvier 2009

- *Il est recommandé à la Confédération de mettre en œuvre la stratégie Cybersanté en épuisant au maximum les compétences juridiques existantes au niveau fédéral. Il faudra se prononcer sur l'éventualité d'une modification de la Constitution dans le cadre des travaux législatifs.*

Recommandation 1 : Epuiser les compétences au niveau fédéral avec une éventuelle modification de la Constitution

Répartition des compétences entre la Confédération et les cantons pour la mise en œuvre de la stratégie nationale en matière de cybersanté

Annexe 5

5.3 Formes possibles de coordination nationale

La coordination entre les activités de la Confédération et des cantons dans le domaine de la cybersanté a été réglée pour la première phase (jusqu'au 31.12.2011) au moyen d'une convention-cadre entre le DFI et la CDS. Cette convention a notamment pour objet la création et l'organisation de l'organe de coordinations de la cybersanté ainsi que la définition des tâches de ce dernier.

Coordination de la mise en œuvre

Pour les phases suivantes du projet, la question se pose de savoir comment coordonner les processus législatifs entre Confédération et cantons d'une part, entre les cantons de l'autre, pour garantir l'introduction homogène du dossier électronique du patient et d'autres applications de la cybersanté. Le canton de Genève, qui dispose déjà d'une base juridique spécifique à la cybersanté (cf. ch. 3.6), a incité, dans le cadre de l'audition, les cantons à mettre à disposition un jeu de réglementations-modèles qui puissent être intégrées dans la législation cantonale. Un tel recueil de textes devrait faciliter l'harmonisation des réglementations cantonales.

Trois types de solution, avec des sous-variantes, s'offrent pour la coordination nationale de la stratégie en matière de cybersanté.

Action coordonnée des cantons

1er type de solution : action coordonnée des cantons

1a) Organe intercantonal fixant des règles de droit

En vertu de l'art. 48 Cst., les cantons peuvent charger un organe intercantonal d'édicter des dispositions intercantonales. Une organisation intercantonale, nouvelle ou existante, à laquelle la Confédération ne participe pas, pourrait se voir attribuer une telle compétence. L'organe de coordination existant se bornerait alors à des tâches de planification et de coordination.

1b) Concordat fixant directement des règles de droit

Il est également possible de créer un droit intercantonal de mise en œuvre de la stratégie de cybersanté au moyen d'un concordat fixant directement des règles de droit. La conclusion d'un tel concordat présenterait pour les cantons l'avantage qu'ils ne devraient pas édicter chacun leurs propres dispositions de mise en œuvre de la stratégie. Les dispositions à régler au niveau cantonal pour l'introduction du dossier électronique du patient pourraient être intégrées dans le concordat ; elles seraient alors contraignantes pour les cantons adhérant à celui-ci. La stratégie en matière de cybersanté pourrait ainsi être introduite par étapes dans ces cantons sans qu'il se forme des systèmes incompatibles entre eux.

1c) Concordat fixant indirectement des règles de droit

Un concordat fixant indirectement des règles de droit pourrait aussi être un moyen d'arriver à une réglementation homogène dans les cantons sans empiéter sur leurs compétences législatives. L'accord intercantonal définirait quels domaines doivent être réglés par les cantons et de quelle manière. Les dispositions seraient, dans une deuxième phase, édictée par les cantons suivant le processus législatif usuel.

1d) Collaboration informelle entre les cantons

Dans l'esprit d'une collaboration informelle, la coordination des procédures législatives cantonales pourrait être assumée par la CDS. La CDS peut élaborer des recommandations à l'intention des cantons et formuler un contenu type des dispositions. De telles recommandations peuvent certes être importantes, mais elles restent non contraignantes.

Action non coordonnée des cantons

2e type de solution : action non coordonnée des cantons

Les cantons édictent les dispositions par le processus législatif usuel, et leur contenu n'est pas harmonisé. Cette façon de faire implique le risque de produire différentes solutions incompatibles entre elles.

Organe de coordination fixant des règles de droit

3e type de solution : organe de coordination Confédération-cantons fixant des règles de droit

Aux termes de l'art. 48, al. 4, Cst., les cantons peuvent, par une convention, habiliter un organe intercantonal à édicter pour sa mise en œuvre des dispositions contenant des règles de droit. La Confédération peut participer à la conclusion de telles conventions ou faire partie d'une organisation intercantonale si celles-ci concernent une matière dans laquelle la Confédération et les cantons disposent de compétences parallèles.

Mais comme tel n'est pas le cas dans le domaine de la santé, une participation de la Confédération à une telle convention ou à un tel organe est exclue. Par conséquent, il n'est pas possible non plus d'habiliter l'organe de coordination existant à édicter des dispositions de mise en œuvre de la stratégie en matière de cybersanté communes à la Confédération et aux cantons.

- *Les cantons complètent les bases légales nécessaires dans le cadre de leurs compétences pour combler les lacunes dans la réglementation fédérale qui résulteraient inévitablement du partage des compétences. Il leur est recommandé de coordonner les efforts en matière de législation cybersanté.*

Recommandation 2 : Combler les lacunes juridiques par une action coordonnée des cantons

Formes possibles de coordination nationale de la mise en œuvre de la stratégie en matière de cybersanté

Annexe 6

5.4 Inscription du dossier électronique du patient dans le droit fédéral

Il s'agit d'établir dans quelles lois fédérales existantes ou, le cas échéant, dans quelles nouvelles lois fédérales des dispositions relatives aux divers thèmes de la cybersanté pourraient être prévues. L'accent est mis sur l'ancrage légal du principe du dossier électronique du patient, car celui-ci constitue la principale application de la cybersanté (à part le portail santé, dont l'ancrage légal est déjà prévu dans la loi sur la prévention).

Inscription dans les lois fédérales existantes ou dans de nouvelles lois

Quatre variantes se dessinent pour l'inscription du dossier électronique du patient dans le droit fédéral. Pour chaque variante, une loi fédérale constitue le point de référence principal. Mais il restera toujours certains aspects à régler dans d'autres lois, ou d'autres lois devront être déclarées applicables, ou des renvois seront nécessaires dans d'autres lois. On pense, p. ex., à l'obligation du prestataire de soins de tenir un dossier, avec un point de référence possible dans la LPMéd.

Quatre variantes

Variante 1 : inscription dans la loi sur l'assurance-maladie (LAMal)

LAMal

Les dispositions concernant le dossier électronique du patient pourraient être intégrées dans la LAMal. Le dossier électronique du patient devrait cependant être clairement séparé des règles relatives au contrôle de l'économicité par les assureurs, car son but est tout autre et il relève exclusivement du domaine des patients et des fournisseurs de prestations. Une possibilité serait d'inscrire ces dispositions dans une section « Dossier du patient » à part, p. ex., dans le chap. 4 « Fournisseurs de prestations » (art. 59*a* ss.). Des renvois à ces dispositions de la LAMal devraient être faits dans les autres lois sur les assurances sociales qui prévoient aussi le remboursement de prestations médicales (LAI, LAA, LAM, évent. LAVS).

La législation sur l'assurance-maladie est déjà dans de nombreux domaines un instrument par lequel la Confédération exerce une influence très générale sur l'économicité et la qualité des prestations fournies dans le domaine de la santé (p. ex., admission à pratiquer à la charge de l'assurance obligatoire des soins, critères uniformes pour l'organisation de la planification hospitalière, etc.). La motivation essentiellement économique avancée pour cela peut également convaincre s'agissant de la mise en place du dossier électronique du patient. Une gestion efficiente

de ce dernier, non limitée à chaque établissement, agit directement sur la qualité du traitement et sur les frais que celui-ci génère. Là où les coûts sont supportés par l'assurance-maladie sociale, la gestion du dossier est en rapport direct avec la question de l'économicité et de l'adéquation des prestations.

La carte d'assuré de l'assurance obligatoire des soins s'offre tout naturellement comme clé d'accès au dossier électronique du patient, moyennant une fonction supplémentaire. Déjà lorsqu'il a inscrit la carte d'assuré à l'art. 42*a* LAMal, le Parlement voulait faire un premier pas en direction d'une carte de santé. L'inscription du dossier électronique du patient dans la LAMal se situerait dans le droit fil de cette tendance.

La nature du dossier électronique du patient concerne toutefois la relation entre prestataires de soins et patient, qui va bien au-delà de l'aspect du droit des assurances sociales. Pour cette raison, le projet partiel « Bases légales » juge qu'il serait plutôt difficile de motiver son inscription dans la LAMal.

Variante 2 : inscription dans la loi sur les professions médicales (LPMéd) LPMéd

La tenue du dossier électronique du patient pourrait aussi être prévue dans la LPMéd. Celle-ci se fonde sur l'art. 95 Cst. et règle la formation et les conditions d'exercice de la profession par les membres du corps médical exerçant dans le secteur privé. L'art. 40 LPMéd énumère les devoirs professionnels des professions comprises dans le champ d'application de la loi. Il s'agit de clauses générales susceptibles d'être précisées. Il serait donc possible de prévoir ici une obligation de documentation étendue, incluant la tenue du dossier électronique du patient.

Une telle manière de faire pose cependant un problème dans la mesure où le champ d'application de la LPMéd est limité pour ce qui est des personnes. Elle ne concerne pour l'heure que les personnes qui exercent une profession médicale universitaire, à titre indépendant, dans le secteur privé. Si, comme il est prévu, une prochaine révision de la loi en étend le champ d'application aux membres du corps médical exerçant dans le secteur privé sous leur propre responsabilité professionnelle, le cercle des professionnels considérés s'élargirait, car il comprendrait aussi les employés d'entreprises privées (p. ex., cabinets de groupe et cliniques privées), mais une grosse lacune subsisterait. En particulier, la loi ne s'appliquerait toujours pas aux membres du corps médical exerçant dans le secteur public, p. ex., aux employés des hôpitaux cantonaux. Les hôpitaux publics sont exclus du champ d'application de l'art. 95 Cst. La Confédération ne peut légiférer sur la base de cet article que sur l'exercice des activités économiques lucratives privées. Les cantons devraient donc édicter des règles analogues pour les groupes professionnels relevant de leur compétence. S'ils ne le faisaient pas, l'obligation de tenir le dossier électronique du patient ne s'appliquerait alors qu'aux membres du corps médical exerçant dans le secteur privé, ce qui causerait une inégalité de traitement par rapport à leurs confrères exerçant dans le secteur public.

Inscrire dans la LPMéd l'obligation de tenir le dossier électronique du patient représenterait aussi, suivant la nature et l'intensité de la réglementation, une ingérence dans la liberté économique. Cette liberté peut

cependant être restreinte dans les limites de la proportionnalité.

Afin d'inclure les professions médicales non universitaires exclues de la LPMéd, il conviendrait d'envisager la possibilité d'une réglementation dans la loi fédérale sur la formation professionnelle (LFPr ; RS 412.10) ou plus tard dans une éventuelle « loi fédérale sur les professions de la santé ». La loi sur la formation professionnelle a pour base constitutionnelle l'art. 63 Cst. (formation professionnelle). Cette voie n'est pas examinée pour l'instant, car le dossier électronique du patient concerne en premier lieu le domaine de la couverture sanitaire et n'a pas grand-chose à voir avec la formation professionnelle.

Variante 3 : inscription dans la loi sur la partie générale du droit des assurances sociales (LPGA) LPGA

On peut se demander si les dispositions relatives au dossier électronique du patient ne devraient pas être fixées dans la LPGA, qui coordonne le droit des assurances sociales. La LPGA règle principalement la relation entre la personne assurée et l'assurance sociale (AVS, AI, PC, LFA, LAFam, AC, AMal, AA et AM). Elle contient les règles de procédure générales, c.-à-d. applicables à toutes les assurances sociales, pour faire valoir droits et obligations (cf. art. 1 LPGA ; RS 830.1). L'art. 32 LPGA règle la fourniture de données en tant qu'assistance administrative pour des procédures de droit des assurances sociales. En revanche, le traitement et surtout la communication de données ne sont pas réglés dans la LPGA, mais dans les différentes lois sur les assurances sociales, car les prescriptions diffèrent d'une assurance à l'autre.

Le dossier électronique du patient concerne avant tout la relation entre prestataires de soins et patient (soins de santé individuels). Seules quelques branches des assurances sociales s'occupent de cette relation au sens le plus large, à savoir l'assurance-maladie, l'assurance-accidents, l'assurance militaire et l'assurance-invalidité. Il ne s'agit donc pas d'un thème général. Si l'on voulait inclure les règles y relatives dans la partie générale du droit des assurances sociales, il faudrait préciser qu'elles ne s'appliquent pas aux autres branches. Le maniement de la documentation relative au patient n'est, au fond, rien d'autre que le traitement de données personnelles. Celui-ci, dans la conception actuelle de la loi, est réglé, on l'a dit, dans les différentes lois sur les assurances sociales. La LPGA n'est le canal qui convient que pour les dispositions qui concernent l'ensemble des assurances sociales. Celles relatives au dossier électronique du patient n'en font pas partie.

Variante 4 : promulgation d'une nouvelle loi-cadre Nouvelle loi-cadre

La promulgation d'une nouvelle loi-cadre fédérale pour l'introduction du dossier électronique du patient peut aussi être envisagée sur la base des compétences fédérales existantes, bien qu'elles soient limitées. Les règles relatives à l'ouverture, à la gestion et au suivi du dossier électronique du patient seraient ainsi clairement séparées de l'application de l'assurance-maladie. Là où les assureurs sociaux devraient être impliqués, des renvois seraient nécessaires. Cette loi spécifique empêcherait que l'assurance-maladie apparaisse comme l'assurance sociale principalement concernée. Tous les assureurs sociaux seraient visés de la même manière en tant qu'agents financeurs. Enfin, les règles relatives au portail sur la santé et aux contenus qui y sont liés pourraient être intégrés dans la nouvelle loi par le biais d'un renvoi dans la loi sur la prévention.

Conçue comme une loi-cadre, la nouvelle loi pourrait contenir les principes et les principales conditions relatives à la tenue du dossier électronique du patient. Ultérieurement, des règles relatives à d'autres applications de cybersanté pourraient aussi y être intégrées.

Etant donné l'étroitesse des compétences que la Constitution fédérale accorde à la Confédération dans le domaine de la santé, il devrait être difficile de justifier la promulgation d'une nouvelle loi fédérale autonome. Cependant, l'édiction d'une « loi-cadre sur la cybersanté » présenterait aussi des avantages significatifs, mettant en évidence l'importance de la cybersanté. Les règles relatives à l'ouverture, à la gestion et au suivi du dossier électronique du patient seraient ainsi clairement séparées de l'application des assurances sociales. Tous les assureurs sociaux seraient visés de la même manière en tant qu'agents financeurs, ce qui ne serait pas le cas, par exemple, en cas de fixation de ces règles dans la LAMal. Une loi conçue comme une loi-cadre réglerait notamment les principes essentiels et les principales conditions cadre, ce qui correspond exactement à la philosophie de base adoptée (voir chap. 4.3 du rapport final).

La loi-cadre devrait être exécutée par la Confédération et les cantons. Les lacunes qui subsisteraient même avec cette solution devraient être comblées dans le droit cantonal.

Après l'audition de mai-juin 2009, la recommandation 3 du projet partiel « Bases légales » a été modifiée sur la base notamment des réponses de l'OFSP et de différents cantons. L'OFSP, qui dirigera le prochain projet législatif, souhaite décider ultérieurement de la forme concrète à donner aux réglementations légales. Vu les modifications apportées, la teneur de la réglementation se borne à dire qu'il faut édicter des règles au niveau du droit fédéral, ce qui correspond pratiquement au contenu de la recommandation 1.

Recommandation 3 : Bases légales

Il est recommandé à la Confédération de promulguer des réglementations en vue de la création de bases légales concernant le dossier électronique du patient. La décision concernant la structure formelle de ces réglementations légales pour le dossier électronique du patient au niveau fédéral (nouvelle loi-cadre / actes modificateurs / modification d'une loi avec adaptations d'autres lois) doit être prise après la première phase des travaux législatifs.

5.5 Forme juridique de l'instance responsable de l'organe de coordination de la cybersanté

Différentes formes juridiques envisageables

Le projet partiel « Bases légales » a examiné quelles formes juridiques entrent en ligne de compte pour l'instance responsable de l'organe de coordination de la cybersanté. Il est apparu que le choix de la forme juridique dépendait dans une mesure déterminante des tâches qui devraient être accomplies et des coûts ainsi impliqués. Suivant les tâches et les objectifs de l'organisation, les exigences relatives aux possibilités de codécision des intéressés, aux aspects essentiels de la gestion de l'organe et aux possibilités de décision de la direction seront différentes. La question de savoir dans quelle mesure des possibilités de prise d'influence politique doivent être maintenues, et comment les garantir le cas échéant, jouera également un rôle déterminant.

Les points suivants doivent être tirés au clair avant que l'on puisse formuler une recommandation sur la forme juridique : Conclusion

- tâches de l'organe de coordination ;
- instance responsable, participation et droits de codécision ;
- organisation de l'organe de coordination.

5.6 Identification, authentification et autorisation

Identification Identification : d'autres travaux sont nécessaires

Les considérations juridiques sur l'identification des patients et des prestataires de soins ne pourront être formulées que quand l'identifiant de chaque groupe aura été défini. Il faut aussi déterminer le responsable de l'identification. L'identification des patients et des prestataires de soins ainsi que le responsable de cette identification devront donc être définis dans les travaux ultérieurs de mise en œuvre de la stratégie.

L'utilisation du numéro AVS en tant qu'identifiant du patient est possible à condition de créer de nouvelles bases légales au niveau des cantons ou de la Confédération. La recommandation du comité de pilotage selon laquelle il faut fixer autant que possible les règles dans le droit fédéral (cf. ch. 5.2) parle en faveur de la création de cette base dans le droit fédéral. Numéro AVS en tant qu'identifiant du patient

Dans les autres travaux visant la mise en œuvre de la stratégie, il faut clarifier s'il est souhaité que le numéro AVS soit utilisé pour l'identification des patients. En cas d'avis favorable, il est recommandé à la Confédération d'envisager une base légale nationale pour utiliser ce numéro comme identifiant du patient, sans toutefois qu'il soit l'unique identifiant. *Recommandation 4 : Disposition fédérale pour l'utilisation du numéro AVS comme numéro d'identification des patients*

Authentification Authentification : d'autres travaux sont nécessaires

Les contenus touchant l'authentification doivent être élaborés dans le cadre des autres travaux de mise en œuvre. Les examens nécessaires pour l'authentification sont, en ce qui concerne les patients, en relation avec le développement de la clé d'accès au dossier électronique du patient et, pour les prestataires de soins, avec celui d'un concept suisse de HPC. En ce sens, ils sont couverts par la recommandation 5.

Autorisation Autorisation : concept d'accès général

Un concept a été introduit dans l'OCA pour l'accès des prestataires de soins aux données personnelles visées à l'art. 42*a*, al. 4, LAMal. Il s'agit maintenant d'élaborer un concept général pour l'accès des prestataires de soins au dossier électronique du patient. La question de son caractère obligatoire et celle de son ancrage légal devront être réglées dans le cadre des autres travaux de mise en œuvre de la stratégie, qui devront donc comprendre l'élaboration d'un concept d'accès général.

5.7 Autres thèmes

Diverses questions relatives à l'ancrage légal des prestations de télémédecine et d'autres domaines connexes ont été soulevées au ch. 4.8. La Questions juridiques ouvertes dans le do-

télémédecine n'est pas un champ d'action prioritaire dans la stratégie cybersanté Suisse, mais celle-ci en tient compte comme d'un sous-domaine de la cybersanté à l'instar d'autres processus. Les projets partiels « Bases légales » ainsi que « Financement et mesures d'incitation » ont cependant abordé le thème de la télémédecine. Il conviendra de définir dans le cadre des travaux ultérieurs ce que l'on entend exactement par « télémédecine », puis de trouver les voies de financement et d'examiner les mesures d'incitation.

maine de la télémédecine

Les paragraphes qui suivent tiennent compte des questions soulevées, sans parvenir à les clarifier. On propose également une manière de procéder.

La Commission européenne (CE) a publié le 4 novembre 2008 une communication concernant l'utilité de la télémédecine pour les patients, les systèmes de santé et la société (COM(2008) 689). Elle y commente les dispositions relatives aux termes employés et propose des mesures de promotion de la télémédecine. Les Etats membres sont instamment priés :

Communication et recommandations de la Commission des communautés européennes du 4 novembre 2008 concernant la télémédecine

- d'évaluer leurs besoins et leurs priorités dans le domaine de la télémédecine d'ici à la fin de 2009. Ces priorités devraient faire partie des stratégies nationales de santé qui seront examinées lors de la conférence ministérielle sur la santé en ligne de 2010 ;
- d'examiner et d'adopter, d'ici à la fin de 2011, leurs réglementations nationales de manière à ce qu'elles permettent un accès plus large aux services de télémédecine. Elles devront aussi couvrir des aspects tels que l'accréditation, la responsabilité civile, le remboursement, la confidentialité et la protection des données.

La Commission entend aussi encourager des mesures prises par ses Etats membres et prendre elle-même des mesures. Elle veut notamment instituer une plateforme d'échange sur les réglementations nationales en vigueur (en 2009) et soutenir l'élaboration de lignes directrices en vue d'évaluer les effets, l'efficacité et l'efficience des services de télémédecine (jusqu'en 2011).

➢ *Il est recommandé à la Confédération et aux cantons d'examiner la mise en œuvre, selon leur domaine de compétences, des mesures publiées par la Commission européenne (télémédecine).*	*Recommandation 5 : Examen de la mise en œuvre des mesures de la CE (télémédecine)*

Dans la prochaine phase de mise en œuvre de la stratégie, l'organe de coordination offre une plateforme pour traiter les questions qui se posent dans le domaine de la télémédecine.

L'organe de coordination, plateforme pour d'autres travaux dans le domaine de la télémédecine

5.8 Conclusions

Les considérations qui précèdent permettent de tirer les conclusions suivantes :

Le processus législatif peut être mis en route au niveau national

- L'interprétation extensive des compétences fédérales recommandée par le comité de pilotage, avec le comblement des lacunes juridiques par une action coordonnée des cantons, offre un garde-fou. Il s'agit maintenant de préparer l'inscription du dossier

électronique du patient dans la loi de telle sorte qu'il subsiste le moins possible de lacunes juridiques.

- Les résultats présentés et les recommandations adoptées permettent à la Confédération d'entamer le processus législatif au niveau national. Les résultats détaillés du projet partiel « Normes et architecture » seront toutefois nécessaires pour les dispositions au niveau des ordonnances.
- Les prochaines étapes des travaux résultent des recommandations 1 à 5 formulées. Il conviendra de redéfinir en partie les compétences relatives aux travaux ultérieurs.

Annexes