ETAT DE FRIBOURG
STAAT FREIBURG

COPIE

Autorité cantonale de la transparence et de la protection des données
Rue des Chanoines 2, 1700 Fribourg

Direction de la santé et des affaires sociales
Secrétariat général
M. Alexandre Grandjean
Conseiller juridique
C é a n s

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

La Commission

Rue des Chanoines 2, 1700 Fribourg

T +41 26 322 50 08, F +41 26 305 59 72
www.fr.ch/atprd

Réf: DNS/mcho doss.n°3038
Courriel: secretariatatprd@fr.ch

Fribourg, le 17 novembre 2011

Loi fédérale sur le dossier électronique du patient (LDEP) – Procédure de consultation au niveau fédéral

Monsieur le Conseiller juridique,

Nous nous référons à votre courrier électronique du 26 septembre 2011 concernant l'objet cité en référence et vous remercions de nous avoir consultés à ce sujet.

La Commission en a traité lors de sa séance du 15 novembre 2011. Elle ne se prononce que sur les aspects relatifs à la protection des données et à la transparence et vous fait les remarques suivantes (art. 30a al. 1 let. b de la loi du 25 novembre 1994 sur la protection des données, LPrD ; art. 40 let. c de la loi du 9 septembre 2009 sur l'information et l'accès aux documents, LInf).

I. Sous l'angle de la protection des données

> La Commission est d'avis que le maintien du rapport de confiance entre le médecin et son patient est primordial et elle rejoint en cela la position de la FMH datée de novembre 2010 (cf. document annexé). Une protection optimale des données permet de maintenir un rapport de confiance entre le médecin et son patient et par là-même un traitement efficace et approprié.

> La Commission estime nécessaire de limiter les droits d'accès et de préciser les principales modalités de cette limitation dans la loi elle-même (art. 4 LDEP). La délégation de compétence au Conseil fédéral doit en particulier préciser que l'accès au dossier électronique du patient est autorisé aux seuls fournisseurs de soins, c'est-à-dire ceux directement impliqués dans le diagnostic et/ou le traitement des patients.

> Pour le reste, la Commission se rallie à la prise de position de Privatim (les commissaires suisses à la protection des données) datée du 14 novembre 2011, dont une copie est annexée à la présente.

II. Sous l'angle de la Transparence

La Commission n'a pas de remarque à formuler.

Tout en vous souhaitant bonne réception de nos remarques et en vous remerciant de bien vouloir nous informer de la suite que vous y donnerez, nous vous prions de croire, Monsieur le Conseiller juridique, à l'assurance de notre parfaite considération.

Marc Sugnaux
Président

Annexes

- Avis de la FMH daté de novembre 2010
- Prise de position de Privatim du 14 novembre 2011

FMH

Verbindung der Schweizer Ärztinnen und Ärzte
Fédération des médecins suisses
Federazione dei medici svizzeri
Swiss Medical Association

L'avis de la FMH

eHealth: il faut préserver le secret médical et la protection des données!

- Le secret médical et la protection des données sont importants car, pour que le traitement soit efficace, le patient doit pouvoir faire entièrement confiance à son médecin.
- Des données sous forme anonyme suffisent pour le contrôle des prestataires de soins ambulatoires. Pour cela, il n'y a pas besoin d'indiquer les diagnostics sur chaque facture.
- Pour le contrôle des hôpitaux sous DRG, l'ajout de données diagnostiques sur la facture n'est pas utile. Le codage ne peut être vérifié de façon appropriée que par une révision externe professionnelle.
- Au sein de l'assurance, des informations médicales détaillées doivent rester exclusivement entre les mains du médecin-conseil.

La situation initiale

Le monde numérique ouvre une multitude de nouvelles possibilités, dans le traitement des patients aussi. Mais simultanément, il donne lieu à une vive discussion sur la protection des données dans ce domaine, moins en ce qui concerne le traitement des patients lui-même, mais principalement à propos de la transmission de données aux assureurs.

Les nouvelles possibilités de transmission et de traitement des données suscitent une envie de données, selon le principe erroné que davantage de données signifie davantage de connaissances, et donc davantage de pouvoir. Pour le traitement des patients, la réalité est tout autre, davantage de données est souvent synonyme de moins d'informations. En effet, quiconque a été une fois confronté aux difficultés rencontrées pour filtrer les données importantes parmi le flux immense de données au sein d'une unité de soins intensifs, le confirmera, tout comme celui qui doit, lors d'une urgence, trouver le plus vite possible les informations essentielles concernant un patient à partir de trois classeurs de son dossier médical.

Les possibilités d'évaluation des données incitent surtout les assureurs à exiger toujours plus de données, sans pour autant fournir un but d'utilisation clair ou même sans pouvoir en démontrer l'utilité.[1]

[1] Sans compter que chaque livraison de données a son prix, qu'il s'agisse d'un prix direct pour la saisie et la livraison des données, ou qu'il s'agisse, à un niveau plus abstrait, du prix que l'on paie pour la divulgation des données et qui peut selon les cas être bien plus élevé.

Elfenstrasse 18, Postfach 170, CH-3000 Bern 15
Telefon +41 31 359 11 11, Fax +41 31 359 11 12
info@fmh.ch, www.fmh.ch

La position de la FMH

Le traitement des patients repose sur la confiance
Pour l'efficacité du traitement, un patient doit pouvoir faire totalement confiance au médecin et être certain que les informations ne tomberont pas en de mauvaises mains.[2] Si le patient ne communique au médecin qu'une partie de ses antécédents, s'il en exclut certaines affections, parce qu'il ne veut pas que d'autres personnes en aient connaissance, alors il peut en résulter un traitement inefficace, voire dangereux.[3] Le législateur, qui a ancré le droit à l'autodétermination informationnelle[4] dans la Constitution fédérale et le secret professionnel dans le Code pénal, était également conscient de ce problème.

La confiance du patient envers le médecin et les membres d'autres professions de la santé ne saurait être imposée – ni par une contrainte de documentation électronique ni par des primes d'assurance plus basses. On ne peut créer cette confiance que si le médecin – et la médecine en général – protège de façon adéquate les informations qui lui sont confiées.

L'eHealth comporte des avantages et des risques
La FMH encourage l'introduction et la mise en application de l'eHealth car la cybersanté offre la possibilité de rendre le traitement des patients plus sûr.

La disponibilité et l'accessibilité accrues des données augmentent toutefois le risque de violation du secret médical et d'utilisation abusive des données. Le facteur humain représente ici le risque le plus important en matière de sécurité. Même une technologie de sécurité sophistiquée et complexe ne peut empêcher totalement que des personnes non autorisées aient accès aux données et en fassent un mauvais usage[5].

C'est pourquoi, dans le domaine de l'économie, les spécialistes en sécurité conseillent à nouveau de conserver uniquement sur papier et de ne pas saisir électroniquement les informations dont la divulgation pourrait menacer la survie de l'entreprise.

Les avantages et les risques diffèrent selon les divers groupes de patients
Les avantages et les risques potentiels de l'eHealth sont différents selon le groupe de patients. Un dossier médical électronique représente un grand potentiel d'avantages, notamment pour les malades chroniques et les patients multimorbides ou ceux suivant un traitement complexe. Toutefois, chez les personnes plus jeunes, le risque d'abus est souvent plus important.

Le risque d'abus est réel
Aux Etats-Unis, on peut acheter des dossiers médicaux pour quelques dollars. Depuis peu, on voit s'installer chez nous des entreprises proposant comme service l'acquisition de données

---

[2] Ce n'est pas un hasard si le secret médical figurait déjà dans le serment d'Hippocrate.
[3] Il faut cependant aussi noter qu'il dépend beaucoup de la personne et de la situation, des informations que le patient considère importantes à protéger. Il y a des personnes qui parlent devant tout le monde de leur maladie psychique; d'autres ne souhaitent en aucun cas que quelqu'un d'autre que le médecin traitant soit au courant de sa maladie. En outre, l'attitude peut changer avec le temps. De plus, ce ne sont pas toujours uniquement des troubles psychiques ou des infections VIH que les patients souhaitent voir traiter de manière confidentielle. On peut penser à la gestion des maladies cancéreuses, il n'y a pas si longtemps. Et parfois, ce sont même des infections banales (du point de vue médical) dont personne d'autre ne devrait avoir connaissance.
[4] Selon l'art. 13 de la Constitution fédérale, toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent. Ce droit fondamental fait partie de la liberté personnelle et inclut le droit à l'autodétermination informationnelle. Ce dernier désigne le droit de tout individu à décider en principe lui-même de la divulgation et de l'utilisation des données qui le concernent.
[5] Récemment, à l'occasion d'une conférence, des experts en sécurité ont émis la recommandation qu'une entreprise devrait «dénumériser» la part vraiment importante et secrète de ses données et ne les conserver que sur papier. Ils ont ajouté que c'était la seule technique vraiment efficace.

médicales. Des fournisseurs de produits médicaux – en Suisse également – ont directement contacté les patients d'un hôpital atteints d'une maladie déterminée. Et – toujours dans notre pays – des employeurs ont eu accès aux données médicales relatives à certaines personnes avant de les engager.

Toute transmission de données concernant un patient doit être motivée
Etant donné que toute remise d'information à des tiers constitue potentiellement une violation du secret médical et pourrait donc porter atteinte à la confiance du patient, toute transmission de données relatives à un patient doit avoir une raison claire. Cela vaut en particulier pour la remise de données aux assureurs. L'assureur est soumis à l'obligation de tenir des dossiers et de constituer des archives.[6] Il doit donc conserver les données qu'il reçoit; la règle prévue par la révision de l'art. 42 al. 3bis de la LAMal, selon laquelle l'assureur devait obtenir les données de facturation mais les conserver sans qu'on puisse établir un lien avec la personne, aurait été inapplicable. Les données stockées chez l'assureur sont potentiellement accessibles à de nombreuses personnes et le changement habituel de personnel, à lui seul, rend impossible de prévoir qui aura accès à ces données dans le futur.

Les informations sensibles ne doivent pas figurer sur les factures
Précisément les factures ne devraient contenir, si possible, aucune information sensible, car elles sont non seulement accessibles à beaucoup de personnes au sein de l'assurance, mais aussi à d'autres personnes et institutions. Selon la situation, les membres de la famille, le curateur, l'aide sociale et les autorités fiscales par exemple peuvent consulter les factures.

eHealth et Managed care
Dans le cadre des discussions sur le Managed care, les assureurs veulent à tout prix imposer le dossier des patients sous forme électronique (dossier patient informatisé DPI) et, en plus, en obtenir l'accès.

La tenue impérative de dossiers patients informatisés et aussi l'accès des assureurs à de tels dossiers rendent les patients «transparents», anéantissent le rapport de confiance entre médecin et patient et signifient, par voie de conséquence, la fin du secret médical.

Là aussi, il importe de clairement séparer les moyens et les buts et de ne pas imposer les moyens. Avec la carte d'assuré, déjà, on a commis l'erreur d'imposer un instrument avant d'avoir clarifié les buts et les processus, ce qui s'est révélé très contre-productif pour le développement et la promotion de l'eHealth. Il faudrait donc éviter de faire la même erreur pour le dossier patient informatisé.

- Le dossier patient informatisé est un *instrument* qui a un but premier: il peut et doit contribuer à la mise en place de processus thérapeutiques sûrs - indépendamment des modèles de soins et d'assurance.
- Aujourd'hui déjà, dans le domaine du Managed care, la majorité des protagonistes travaillent avec des éléments du dossier patient informatisé. Pourtant, cela n'a aucun sens de vouloir imposer un instrument déterminé, à savoir le dossier patient informatisé, pour atteindre un but tel que la promotion du Managed care. Le Managed care doit être encouragé par l'introduction d'incitatifs appropriés à ce système, par exemple par une meilleure compensation des risques, une participation aux frais différenciée, etc.

Au demeurant, ces dernières années, beaucoup d'hôpitaux ont introduit des dossiers patients informatisés. Ce processus a été accéléré par les DRG, mais n'a pas été imposé avec les DRG.

[6] Conformément à la loi sur les archives, l'assureur social ne doit plus remettre aux archives les données nécessaires.

Les propositions de la FMH

Contrôle des prestataires de soins à l'aide de données anonymisées
La livraison systématique de données médicales détaillées personnelles aux assureurs n'est nécessaire ni pour le contrôle des prestataires de soins ambulatoires ni pour celui des hôpitaux et des homes. Des données sous forme anonyme suffisent pour le contrôle des prestataires de soins ambulatoires. Il n'y a pas besoin, pour cela, d'indiquer les diagnostics sur chaque facture.
Pour la vérification des hôpitaux également, il n'est pas indispensable que des données détaillées figurent sur les factures particulières. Les statistiques médicales de l'Office fédéral de la statistique sont la preuve qu'on peut établir les profils des hôpitaux même avec des données anonymes.

Révision externe du codage dans le domaine SwissDRG
Personne ne conteste qu'un contrôle approprié du codage est nécessaire pour les factures DRG. Mais il n'est pas utile d'ajouter des indications diagnostiques sur la facture. La vérification du codage demande un accès au dossier médical complet; l'échantillon doit se rapporter à tous les patients hospitaliers. Par conséquent, le codage ne peut être vérifié de manière appropriée que par une révision externe et professionnelle. Cette vérification doit être opérée par des tiers mandatés d'un commun accord. En effet, il est impensable d'accorder l'accès aux dossiers médicaux aux employés d'un seul assureur au sein de l'hôpital pour qu'ils y effectuent des contrôles et, d'autre part, les échantillons doivent prendre en compte tous les patients d'un hôpital.

Le médecin-conseil en tant que filtre
C'est au médecin-conseil qu'il appartient, dans un cas particulier, de demander les informations médicales détaillées nécessaires et de les évaluer pour l'assureur. L'expérience montre que, dans un tel cas, le médecin-conseil a en premier lieu besoin des résultats d'examens et des rapports (d'opérations, de sortie, etc.) et non pas de données diagnostiques selon la CIM 10. Cela confirme que le fait d'indiquer systématiquement de façon détaillée les diagnostics et d'autres données très personnelles sur les factures n'est ni approprié, ni indispensable et encore moins conforme au principe de la proportionnalité.

Informations complémentaires:
Bulletin des médecins suisses 38/2010: «Lorsque le diagnostic devient un bien commun»
Bulletin des médecins suisses 34/2010: «La révision du codage externe et professionnelle permet de garantir la protection des données»
Prise de position relative au rapport du groupe d'experts eHealth

Berne, novembre 2010

Renseignements:
Jacqueline Wettstein, responsable de la communication de la FMH
Tél. 031/359 11 50, e-mail: jacqueline.wettstein@fmh.ch

privatim
die schweizerischen datenschutzbeauftragten
les commissaires suisses à la protection des données
gli incaricati svizzeri della protezione dei dati

Monsieur
Eric Beer
Office fédéral de la santé publique
Division Projets multisectoriels
3003 Berne

Zurich, le 14 novembre 2011

Consultation sur la nouvelle loi sur le dossier électronique du patient

Monsieur,

Nous vous remercions de nous avoir consultés et vous adressons les remarques ci-dessous sur le projet de loi mentionné en objet.

Compétences législatives de la Confédération
La cybersanté représente un enjeu national et une coordination est nécessaire afin que n'émergent pas des projets isolés qui s'avéreraient incompatibles entre eux. Des normes et des pratiques unifiées s'imposent de manière évidente. La Confédération et les cantons ont d'ailleurs adopté la convention-cadre du 6 septembre 2007, dans le souci d'assurer la meilleure coordination possible. Le projet de loi répond aussi à cet objectif. Même s'il ne s'agit pas d'une question de protection des données, nous vous invitons à examiner à nouveau de manière critique la question des compétences législatives de la Confédération.

Délégation de compétences
De manière générale, le projet de loi contient des normes de délégation larges en faveur du Conseil fédéral. De telles délégations sont en partie nécessaires dans ce domaine très technique. On se trouve toutefois dans un champ de tension avec les principes applicables en matière de protection des données, qui exigent des bases légales formelles d'une certaine densité normative s'agissant du traitement de données sensibles. Il conviendrait d'examiner plus minutieusement chacune des normes de délégation pour déterminer dans quelles mesures les conditions mises à la délégation sont remplies et si elles doivent être précisées.

Consentement (article 3 LDEP)
Nous saluons l'affirmation du caractère volontaire de l'adhésion au système du dossier

privatim
c/o Datenschutzbeauftragter des Kantons Zürich
Postfach, CH-8090 Zürich
Tel. +41 (43) 259 39 99, Fax +41 (43) 259 51 38
praesident@privatim.ch, www.privatim.ch

électronique du patient. Dans le but de promouvoir ce système, on peut toutefois imaginer la constitution de modèles d'assurance maladie obligatoire qui obligeront *de facto* les patients à adhérer au système du dossier électronique. Le caractère volontaire consacré par la loi risque ainsi de se transformer en farce. Nous vous invitons à examiner comment garantir un consentement qui en reste véritablement un.

La loi ne précise pas comment et par qui seront gérées les déclarations de consentements données par les patients. Le message dit que « les déclarations et les révocations de consentement sont gérées par le professionnel de la santé appartenant à la communauté dans laquelle le patient a donné son consentement à la constitution d'un dossier électronique » (p. 43). Il est selon nous souhaitable que les responsabilités apparaissent au niveau de la loi.

Droits d'accès et confidentialité (article 4 LDEP)

L'octroi des droits d'accès et leur gestion constituent un élément central du dossier électronique du patient. Le projet de loi délègue au Conseil fédéral la compétence de régler les modalités d'attribution des degrés de confidentialité et des droits d'accès (art. 4 al. 2 LDEP). La délégation de compétence au Conseil fédéral est très large et peu cadrée. Nous pensons que les degrés de confidentialité doivent être précisés dans la loi. Par ailleurs, on devrait trouver dans la loi une description au moins succincte des modalités dont il est question.

Le droit d'accès à ses propres données est garanti par l'article 4 alinéa 1er lettre a LDEP. Là encore, on ne sait qui assume les responsabilités : Qui assure l'existence d'un portail d'accès électronique certifié ? Qui assume la responsabilité en cas d'impossibilité d'accès ?

On ne sait pas non plus comment et à quelles conditions les patients peuvent accéder aux fichiers de journalisation des accès (*logfiles*). Sans prôner une centralisation de ces fichiers, on doit tendre à un système qui permette facilement aux patients de savoir qui a consulté les données les concernant. Les patients devraient ainsi pouvoir s'adresser à un prestataire (par exemple la communauté à laquelle le patient a donné son consentement), charge à celui-ci de réunir les *logfiles* existants.

Nous approuvons l'obligation d'informer en cas d'accès à des données en cas d'urgence médicale. La loi doit toutefois préciser qui a la responsabilité de cette annonce.

Identification (article 5 LDEP)

Les dossiers électroniques des patients peuvent concerner tant des personnes à qui un NAVS13 a été attribué que des personnes qui n'en ont pas (encore) (p. ex. : nouveaux nés, personnes étrangères). La personnalité des uns et des autres mérite d'être également protégée. Il est donc nécessaire d'adopter pour chacun des groupes des identificateurs répondant à des normes sévères de sécurité. Pour les personnes qui en disposent, le NAVS13 est un attribut parmi d'autres. Pour celles qui n'en ont pas, on doit définir un set d'attributs sans NAVS13. Dans les deux cas de figure, on doit pouvoir identifier de manière sûre les identités des personnes au moyen d'une procédure d'identification unifiée.

Le deuxième set pourrait être utilisé également pour les personnes disposant d'un NAVS13. On créerait ainsi, par une procédure unique, un identifiant sûr pour l'ensemble des patients, indépendamment du numéro d'assurance sociale. Le NAVS13 n'étant pas

un caractère nécessaire - il ne permet pas d'identifier les personnes qui n'en ont pas, il ne devrait par conséquent pas être mentionné dans le projet de loi.

Le message mentionne la carte d'assuré telle qu'elle apparaît à l'article 42a LAMal. Or cette carte ne saurait servir de support à un identifiant en l'état actuel. Cette fonction n'est d'une part pas mentionnée dans la LAMal. D'autre part, il ne serait pas admissible que ce soient les assureurs qui attribuent un identifiant sur une carte fournie par leurs soins. Si le message mentionne qu'il s'agirait d' « une carte d'assuré plus élaborée », on manque de précisions sur les orientations auxquelles on peut s'attendre. Le message doit à cet égard également être plus explicite.

Contenu
Le dossier électronique du patient comprendra des données « qui sont pertinentes pour le traitement d'un patient » (art. 2 al. 1er let. a LDEP). Si l'on peut concevoir qu'il soit difficile de préciser dans la loi elle-même les données dont il s'agit, le message pourrait détailler le type de données qu'on envisage d'intégrer, en l'état de la réflexion. La formulation choisie ouvre en effet un champ d'interprétation extrêmement large qui mérite d'être précisé.

Sécurité et certification (articles 7 à 10 LDEP)
La sécurité des données est essentielle s'agissant du dossier électronique des patients. Le projet de loi en tient compte en prévoyant une obligation de certification (art. 7 LDEP). Le soin de fixer les critères est laissé au Conseil fédéral (art. 8 LDEP). Nous partons du principe qu'il sera tenu compte des exigences en matière de protection des données.

Il ressort du message que l'attribution des droits d'accès se fera en principe en faveur de personnes, de manière nominative. Ce principe doit être précisé dans la loi. Si au contraire on envisage de permettre l'attribution de droits à des groupes de personnes, la loi doit le prévoir expressément en fixant des critères ouvrant cette possibilité.

Nous vous adressons, Monsieur, nos meilleures salutations.

Bruno Baeriswyl
Président de privatim