

## Télématique médicale

Doc	a076016
Date de publication	15/02/1997
Origine	NR
	Informatique
	Secret professionnel
Thèmes	Vie privée
	Responsabilité du médecin
	Prescriptions

Le Centre de recherches "informatique et droit" des Facultés universitaires Notre-Dame de la Paix communique au Conseil national des questions posées par l'introduction de la télématique dans le domaine de la santé et leur demande de répondre à un questionnaire qu'il a établi à ce sujet.

### Réponse du Conseil national :

Me référant à votre lettre du 31 juillet 1996, je vous prie de trouver, en annexe, les réponses que le Conseil national de l'Ordre des médecins a données à votre questionnaire, lors de sa séance du 15 février 1997.

## QUESTIONNAIRE - ASPECTS LEGAUX DE LA TELEMATIQUE MEDICALE

### 1. Réglementations

A l'heure où l'on évolue vers la transmission électronique des données médicales, il est nécessaire de procéder à une analyse détaillée des aspects légaux et des problèmes de sécurité en matière de télématique médicale.

1.1. Existe-t-il dans votre pays une législation réglementant la transmission électronique des données médicales sur réseau ?

*NON*

1.2. S'il existe un organisme chargé de la protection de la vie privée, s'est-il positionné par rapport à l'informatisation des données médicales et à leur circulation sur réseau ?

*NON*

1.3 L'Ordre des médecins et/ou des organisations professionnelles ont-ils adopté des règlements ou des recommandations relatifs aux problèmes de sécurité liés à la communication électronique des données médicales ?

*OUI*

1.4. Si la réponse aux questions précédentes est oui, quels sont les points principaux de ces réglementations ? Pourriez-vous nous communiquer les textes dont vous

disposez à ce sujet ?

*Le Conseil national s'est préoccupé depuis plusieurs années du respect de la confidentialité des données médicales transmises par voie électronique. Il a émis plusieurs recommandations dont les textes sont joints :*

*Avis du Conseil national*

*du 16 octobre 1993 - Bulletin n° 63, mars 1994, page 19.*

*du 16 avril 1994 - Bulletin n° 65, septembre 1994, page 22.*

*du 22 avril 1995 - Bulletin n° 69, septembre 1995, page 13.*

## 2. Mesures de contrôle ; autorités compétentes

La fiabilité des systèmes télématiques en matière médicale dépendra, d'une part du système de contrôle d'accès mis en oeuvre et, d'autre part, de la gestion des clés cryptographiques ainsi que de la procédure de certification.

2.1. Comment est organisé le **contrôle** (technique, gestion) de **l'accès** aux données médicales informatisées ?

*Les médecins qui souhaitent participer à un système de courrier électronique et échanger des données médicales doivent être enregistrés auprès de leur conseil de l'Ordre provincial. Le rôle du conseil consiste à certifier l'identité des participants ainsi que l'authenticité des clés publiques qui leur sont attribuées. L'accès aux données médicales informatisées est contrôlé par un code d'accès propre à chaque médecin. Le système doit être organisé de manière telle que seul le médecin en charge d'un patient puisse avoir accès aux données de ce dernier.*

2.1.1 Existe-t-il un système de carte professionnelle santé matérialisant l'accès au réseau ?

*NON*

Si oui, comment ce système est-il mis en oeuvre ?

2.1.2. Existe-t-il un organisme indépendant (un "Trusted Third Party") qui serait chargé de veiller au bon déroulement des transmissions de données électroniques dans le domaine de la santé ?

*OUI*

Si oui,

- quelle est la position du Conseil de l'Ordre face à cet organe ? Le Conseil national envisage d'exercer la mission de mandataire de confiance au nom des dix conseils provinciaux.
- qui sont ses membres ? Le Conseil de l'Ordre est un organisme de droit public créé par l'arrêté royal n° 79 du 10 novembre 1967. Il se compose de dix membres médecins élus par les dix conseils provinciaux, de six membres médecins nommés par le Roi sur proposition des Universités et est présidé par un magistrat de la Cour de Cassation.
- quelles sont ses compétences ? Ses compétences sont déterminées par la loi (A.R. n° 79 du 10 novembre 1967), elles comprennent notamment l'élaboration d'un Code de déontologie médicale.

2.3. Existe-t-il un organisme exerçant les compétences suivantes :

- a. l'habilitation, selon la catégorie professionnelle, des professionnels pouvant avoir

accès aux données médicales informatisées ;

*NON*

*Dans notre conception éthique chaque médecin établit à lui seul un dossier médical pour chaque patient. Il est responsable de sa conservation.*

Seuls les médecins appelés à donner des soins aux malades peuvent y avoir accès. Ceci est valable également pour les données médicales informatisées. Des projets récents de dossier médical global prévoient également la centralisation des données auprès d'un seul médecin. L'accès à ces données ne peut se faire que conformément aux dispositions légales en vigueur.

- b. la distribution des clés cryptographiques (c.-à-d. de la clé "publique" destinée à décrypter les messages encodés en utilisant la clé "privée" de l'expéditeur) aux professionnels de santé ;

*NON*

*Il n'existe pas à ce jour d'organisme de distribution. Le Conseil national se propose d'assumer la fonction de certification des clés.*

- c. la délivrance et la personnalisation des cartes professionnelles santé;

*NON*

*La délivrance de cartes professionnelles et susceptibles de comporter un code d'accès aux données informatisées n'existe pas à ce jour en Belgique. Les conseils provinciaux ont la charge de dresser le Tableau des médecins inscrits après avoir, notamment, vérifié leur titre professionnel. La délivrance des cartes professionnelles médicales est dès lors de leur compétence.*

- d. la certification du lien entre une clé "publique" et un individu déterminé.

*NON, la certification peut être réalisée au sein du Conseil de l'Ordre.*

2.4. Pourriez-vous nous envoyer des documents relatifs aux autorités visées ci-dessus et/ou aux mesures de contrôle mises en oeuvre dans votre pays ?

*Statuts et les arrêtés royaux relatifs à l'Ordre des médecins.*

2.5. Disposez-vous de certains éléments permettant d'établir qui sera considéré comme responsable dans les cas suivants :

2.5.1. accès au réseau sans autorisation préalable ;

*Est responsable celui qui n'a pas pris les précautions nécessaires pour protéger les données et leur accès, en l'occurrence les médecins responsables de l'application des mesures de sécurité.*

2.5.2. délivrance d'un faux certificat.

*L'auteur du faux certificat.*

2.5.3. Si la réponse aux questions précédentes est oui, pouvez-vous préciser ?

*Voir commentaire aux nos 2.5.1. et 2.5.2.*

### 3. Valeur probante des documents électroniques

Alors qu'actuellement seulement une minorité de personnes ne maîtrise l'utilisation des nouvelles technologies, certains experts affirment cependant que les documents électroniques et les signatures digitales peuvent être au moins aussi fiables que les écrits et les signatures manuelles. C'est la raison pour laquelle les techniques digitales

peuvent être envisagées tant pour accroître la validité des données médicales informatisées que pour l'archivage de ces données.

3.1. Dans votre pays, accorde-t-on une certaine valeur probante aux documents électroniques ?

*NON*

*Il faut distinguer :*

- *l'ordonnance médicale, c.-à-d. la prescription de médicaments : le médecin doit signer de sa main son ordonnance conformément à la loi sur les prescriptions médicales (article 15 de l'arrêté royal du 31 mai 1885 approuvant les nouvelles instructions pour les médecins, pour les pharmaciens et pour les droguistes). Une ordonnance électronique non signée n'est pas acceptée à ce jour.*
- *les autres types de documents médicaux : les documents électroniques pourraient être considérés comme un début de preuve.*

3.2. La signature électronique dispose-t-elle de la force probante ?

*NON*

3.2.1. Si oui, quelles sont les exigences minimales en matière de signature électronique ?

3.2.2. Si non, quelles seraient ces exigences minimales en matière de signature électronique ?

*Pour garantir les fonctions possibles de la signature électronique dans un système ouvert où le message suit un long chemin entre différents services et parcourt divers réseaux, les exigences suivantes s'imposent :*

- *L'utilisation d'un système d'encryptage double faisant appel à un algorithme fiable.*
- *Le recours à des systèmes de protection des clés secrètes.*
- *Dans le cas de documents médicaux, un système de depositaire fiable des clés secrètes (key escrow) doit être réalisé.*
- *Vu le caractère transfrontalier des flux électroniques, l'élaboration de règles uniformes pour la confection et l'utilisation de signatures électroniques.*

3.3. Un système d'archivage des données est-il organisé au niveau national ?

*NON*

Si oui, qui en assure la gestion ?

## 4. Internet

4.1. L'accès au réseau sera-t-il possible par Internet ?

*OUI, étant donné le caractère public du réseau, des précautions particulières devront être prises.*

4.2. Quelle est la position de l'Ordre des médecins face à :

4.2.1. la circulation des résultats et examens médicaux sur Internet

4.2.2. la circulation des dossiers médicaux sur Internet :

*Les mêmes règles sont d'application pour les points 4.2.1 et 4.2.2, à savoir :*

- *les règles de déontologie médicale s'appliquent : quant à la confidentialité, expéditeur et destinataire doivent être des médecins ;*
- *le médecin conclura une convention avec une société organisatrice de distribution du courrier électronique, suffisamment indépendante pour éviter tout monopole ou fidélisation; cette convention devra être approuvée par le Conseil provincial ;*
- *le médecin utilisera le système de double clé, les clés seront générées par le médecin sur un P.C. déconnecté de tout réseau ;*
- *le médecin est tenu de vider le plus tôt possible le serveur de tout message.*
- *tout courrier non relevé du serveur doit être effacé endéans le mois.*

4.3. Comment l'Ordre des médecins envisage-t-il de sécuriser l'accès dans ces cas-là ?

*Le Conseil national de l'Ordre des médecins se propose comme "Trusted Third Party" ; comme tel il acceptera et conservera , de façon dûment protégée, les clés publiques et privées des médecins utilisateurs : l'Ordre rendra les clés disponibles en cas de disposition légale ou si nécessaire en cas de décès d'un médecin utilisateur.*