Sites Internet de médecins

Doc	a082002
Date de publication	20/06/1998
Origine	NR
Thèmes	Secret professionnel Publicité et réclame Internet

Le Conseil national émet l'avis ci-dessous au sujet de l'exploitation d'un website par des médecins :

Exploitation d'un website par des médecins

La création d'un site Internet peut répondre à diverses motivations telles par exemple de faire connaître ses coordonnées ou encore d'échanger des informations. Alors qu'initialement le réseau Internet s'est développé dans un but d'échanges entre institutions scientifiques, la majorité des sites actuels affichent des préoccupations essentiellement commerciales.

Il apparaît sur Internet un nombre de plus en plus important de sites reprenant les nom et adresse, lieu de travail et parfois des informations plus spécifiques concernant des médecins (curriculum vitae, publications, photos, etc.) .
Certains font apparaître leurs coordonnées à titre individuel. D'autres, et c'est le cas le plus fréquent actuellement pour les médecins spécialistes, le font au sein d'un site plus global élaboré au nom d'une société scientifique ou d'une institution de soins.
En effet, des cliniques ou hôpitaux élaborent également des sites qui reprennent les listes des médecins avec leur spécialisation, en général présentées sans ostentation. Malheureusement ces listes de médecins sont souvent entourées d'autres textes et/ou photos publicitaires.

De nombreux sites contiennent des références à des sociétés commerciales (logos ou textes), qu'il s'agisse de sociétés pharmaceutiques ou d'autres.

Le Conseil national rappelle que les annonces des médecins ne peuvent avoir de but commercial et que les sites qu'ils créent ne peuvent revêtir d'aspect publicitaire.

Le Conseil national estime que les indications autorisées sur un site Internet sont les nom et prénoms, les titres légaux, la spécialité pratiquée et les mentions qui facilitent les relations du médecin avec ses patients.

Le Conseil national est d'avis qu'un logo peut être apposé à condition d'être discret dans la forme et le contenu.

Le Conseil National rappelle également ses avis relatifs aux mesures destinées à garantir la confidentialité des données couvertes par le secret médical et transmises par voie numérique, qu'il s'agisse d'une messagerie électronique ou du réseau Internet :

- Transmission de courrier par la voie télématique : Bull. 63--p. 21,
- Boîte aux lettres électroniques - Laboratoires : Bull. 63--p. 19,
- Messageries électroniques : Bull. 65--p. 22,
- Communications électroniques : Bull. 69--p. 13

Pour ce qui est des informations non personnelles diffusées sur un site consacré à la médecine, les règles de discrétion et de prudence décrites à l'article 16 ainsi que les interdictions relatives à la collusion avec des tiers prévues aux articles 173 et 174 du code de déontologie sont d'application.

Boîte aux lettres électroniques - Laboratoires

Avis du Conseil national du 16 octobre 1993 :

Transmission de données médicales par voie électronique

La transmission des résultats, documents et d'une façon générale de toute donnée ou communication d'ordre médical, doit se conformer aux principes et garanties que sont l'authenticité, la fiabilité et la confidentialité.
Le médecin est responsable de la préservation du secret médical. La transmission de données médicales ne peut donc s'effectuer que si le médecin a pris toutes les précautions nécessaires à la protection du secret. Les conseils provinciaux de l'Ordre des médecins doivent veiller au respect du secret professionnel en toute circonstance.
La transmission de données médicales par téléfax, modem ou réseau, doit être protégée, tant en ce qui concerne l'accès et l'utilisation que le transport, par des méthodes d'efficacité démontrées, conformes au niveau actuel des connaissances dans ce domaine.

A titre d'exemple :

1. La transmission de résultats ou protocoles par téléfax n'appelle aucune objection d'ordre déontologique, pour autant qu'elle s'opère avec la circonspection qui s'impose comme pour tout échange de correspondance. S'agissant d'une transmission de médecin à médecin, les précautions doivent être prises pour éviter l'accès non autorisé (adressage erroné, contrôle de l'accès,...).

2.1. En ce qui concerne la transmission directe par modem, entre deux médecins, les mêmes précautions doivent être prises.

2.2. Dans le cas d'un système reliant plusieurs utilisateurs, il existe un danger réel d'infractions à la déontologie, notamment de violation du secret médical, de limitation du libre choix du patient ou encore d'octroi d'avantages prohibés, susceptibles de masquer une dichotomie. Une organisation adéquate de la transmission des données permettrait d'éviter ces infractions. Ce mode de transmission ne peut être autorisé que moyennant l'approbation du conseil provincial auquel ressortissent les médecins qui l'utilisent.

Lorsqu'une société ou un médecin souhaite mettre directement, par modem, à la disposition des médecins qui s'adressent à eux, les résultats ou protocoles stockés dans leur ordinateur, ils ne peuvent le faire qu'à la condition d'en avoir fixé l'usage dans un règlement écrit, porté à la connaissance des médecins utilisateurs et approuvé par le conseil provincial de l'Ordre auquel ressortissent ces derniers.

Ce règlement doit garantir le libre choix du médecin et du malade ainsi que le recours, pour assurer la confidentialité, à des méthodes valables permettant le contrôle de l'accès, de la communication, du transport et de l'utilisation des données. Ce règlement doit donc mentionner explicitement le ou les systèmes de sauvegarde prévus pour satisfaire à ces contrôles. Il doit également résulter du règlement que les précautions

nécessaires ont été prises en vue d'éviter les infractions à la déontologie. Un médecin ne peut utiliser ce service qu'après avoir reçu un exemplaire du règlement et obtenu l'approbation du conseil provincial dont il relève.

2.3. Les mêmes précautions doivent être respectées lorsque des données médicales sont stockées dans un ordinateur serveur par différents utilisateurs et peuvent être appelées par les destinataires via leurs propres terminaux (système de "boîte postale électronique"). Il doit apparaître que seul le médecin qui a adressé le patient pour un examen déterminé peut avoir accès aux résultats de son patient et qu'il ne peut obtenir que les données relatives à ses propres patients. Inversement, l'accès au dossier médical tenu par le médecin ne peut être possible. Pour que le libre choix du patient soit respecté, il doit ressortir du règlement que l'usage de ce service n'entraînera pas la création d'un lien illicite entre le médecin et l'initiateur du service. Ce service doit être mis à la disposition de tous les médecins qui souhaitent y recourir sans aucune obligation pour eux d'une collaboration avec un médecin ou service médical déterminé. L'usage de ce mode de transmission de données médicales ne peut procurer au médecin traitant d'autre avantage que celui d'une communication meilleure et plus rapide des résultats.

3. Pour ce qui est de la communication des informations médicales au moyen d'un réseau, par exemple en institution de soins, les mêmes précautions doivent être prises pour sauvegarder la protection et la sécurité des données médicales. Les méthodes utilisées devront répondre aux critères d'efficacité actuels et les mesures prises seront traduites en instructions claires, cohérentes et non ambiguës, dans un règlement interne dont l'application et le contrôle seront confiés à un médecin responsable.

Pour toute forme de transmission de données médicales par voie électronique, le médecin traitant doit avoir la possibilité, s'il le souhaite, d'obtenir confirmation écrite des données transmises.

Transmission de courrier par la voie télématique :

Avis du Conseil national du 16 octobre 1993

Vous trouverez ci-joint l'avis du Conseil national en matière de transmission des données médicales par voie électronique.

L'installation d'un système de communication de courrier par la voie "télématique" (modem) doit être fixée dans un règlement écrit, porté à la connaissance des médecins utilisateurs et approuvé par le Conseil provincial auquel ressortissent ces derniers.

Voir l'avis : "Transmission de données médicales par voie électronique", p. 8.

Messageries électroniques

Avis du Conseil national du 16 avril 1994 :

L'attention du Conseil national a été attirée sur l'existence de la promotion et de l'exploitation de divers systèmes de messagerie électronique dans des conditions non conformes aux règles déontologiques.
Il s'agit d'une part de la vente ou de la mise à la disposition de médecins généralistes de matériel de communication (Modems et programmes) par des laboratoires ou des sociétés agissant pour compte de laboratoires, voire même d'hôpitaux, dans des conditions qui entraînent, pour les destinataires du courrier l'avantage de la disposition rapide des résultats, mais pour les expéditeurs l'avantage de la fidélisation obligée des médecins traitants dont le libre choix se trouve de la sorte limité.

D'autre part, les conditions techniques de cette transmission de données médicales ne garantissent pas, dans beaucoup de cas, le respect de la confidentialité. En effet,

l'accès aux données n'est souvent protégé que par un simple mot de passe, ce qui est notoirement insuffisant sur le plan de la sécurité.

L'avis émis le 16 octobre 1993 par le Conseil national au sujet de la "Transmission de données médicales par voie électronique" affirme très clairement l'interdiction, lors de la transmission par Modem, de l'octroi d'avantages prohibés. De même, s'il y a été indiqué que la confidentialité doit être assurée par des méthodes valables, le Conseil, pour d'évidentes raisons de compétence, s'est abstenu de préciser ces méthodes mais a toutefois chargé les Conseils provinciaux de les contrôler via l'examen des conventions. Cet avis a été publié dans le Bulletin n° 63 Vol. III de mars 1994.

Conscient de la difficulté pour les Conseils provinciaux d'apprécier si les technologies utilisées garantissent le respect des prescrits déontologiques, le Conseil national croit opportun de faire les rappels et suggestions suivantes :

1. Il importe de rappeler aux médecins l'obligation de conclure une convention dont le projet doit être préalablement soumis au conseil provincial. Leur attention doit être attirée sur les aspects déontologiques de ce mode de messagerie.
2. Lorsqu'il s'agit d'apprécier une convention entre un médecin et une organisation ou un établissement de soins dont l'activité s'étend sur plusieurs provinces, il est souhaitable que l'étude du contrat émis par l'institution ou la société exploitant le système soit confiée au conseil de la province dans laquelle celle ci est établie. Il appartient à ce dernier conseil d'informer et de transmettre ses conclusions, le cas échéant via le Conseil national, aux conseils des autres provinces concernées.
3. Il est suggéré de ne pas accepter des systèmes de messagerie dont l'accès serait limité, pour ce qui est des expéditeurs, à un groupe ou un établissement de soins donnés, comme par exemple un seul laboratoire ou un seul hôpital, ce qui pourrait dès lors rendre d'une ou d'une autre manière les médecins demandeurs d'investigations dépendants ou fidélisés. Ceci revient à donner la préférence à des sociétés indépendantes qui accepteraient le courrier émanant de tout demandeur.
4. Les conditions de sécurité minimales indispensables lorsque l'échange de données se fait au sein d'un groupe d'utilisateurs doivent comprendre :
    - un code d'accès, régulièrement modifié, voire même choisi par l'utilisateur;
    - l'encryptage des données au niveau du PC de l'expéditeur, en utilisant une technique dont la fiabilité est reconnue, et dont la description et les références doivent être fournies;
    - l'effacement des données de l'ordinateur serveur central lorsque celles ci ont été transmises et reçues. Les duplicata éventuels seront demandés à l'expéditeur;
    - le décryptage dans le PC du destinataire.

Signalons aussi qu'un Conseil provincial confronté avec ce problème, a exigé la réalisation d'un audit par une société indépendante, à charge du demandeur. Cette procédure a l'avantage d'éviter pour le conseil les difficultés entraînées par ce contrôle essentiellement technique tout en lui fournissant un rapport technique indépendant et valable.
Il serait judicieux également d'exiger que les nombreux logiciels "médicaux" qui sont présentés sur le marché comprennent d'origine un programme valable d'encryptage décryptage.

Communications électroniques - Secret médical

Avis du Conseil national du 22 avril 1995 :

1. Le Conseil national s'est penché sur le problème du respect du secret professionnel lors de la transmission de données couvertes par le secret, par l'entremise d'une boîte

aux lettres électronique.

Lettres et avis du Conseil national envoyés aux Présidents des Conseils provinciaux et des Conseils d'appel :

En sa séance du 22 avril 1995, le Conseil national a adopté le texte dont copie ci-jointe des recommandations relatives à la protection de la confidentialité lors de la transmission de données couvertes par le secret médical par l'entremise d'une boîte aux lettres électronique.

Il vous saurait gré de bien vouloir lui faire connaître votre avis sur les modalités d'application des points 5 et 6, alinéa 1er.

Recommandations relatives à la protection de la confidentialité lors de la transmission de données couvertes par le secret médical par l'entremise d'une boîte aux lettres électronique

Le médecin a l'obligation, conformément à l'article 458 du Code pénal, de respecter le secret médical. La transmission par voie électronique de courrier contenant des données à caractère personnel n'échappe pas à cette obligation légale et déontologique.

1. Seul un médecin, personne physique, peut transmettre et recevoir des données médicales couvertes par le secret professionnel du médecin.
   Au sein d'une institution, le médecin qui transmet ou reçoit des données médicales, ne peut le faire qu'en son nom.
2. Un système à double clé, encore dénommé système mathématique asymétri¬que, assure une sécurité satisfaisante.
3. Afin de préserver leur caractère secret, le médecin devra générer lui-même sur son ordinateur personnel les clés qui lui sont propres. Lors de cette manoeuvre, cet ordinateur ne peut être en connexion avec le réseau.
4. L'accès à la clé secrète est strictement limité au seul propriétaire de celle-ci. Cet accès sera protégé par un mot de passe qui ne pourra être communiqué.
5. Une copie de la clé secrète sera transmise sur disquette par le médecin au Conseil de l'Ordre dont il relève. L'accès à cette disquette sera protégé par une phrase ou un mot de passe conservé séparément sous enveloppe scellée.
6. La clé publique et une "empreinte numérique" de celle-ci, signée par le Conseil de l'Ordre, pourront être transmises à une société organisatrice de la distribution du courrier électronique.
   Cette société devra s'engager à ne communiquer cette clé publique qu'aux seuls médecins qui participent aux échanges de données médicales couvertes par le secret. Elle prendra toutes les mesures pour éviter l'emploi de cette clé à d'autres fins.

7. Il est souhaitable que ces clés publiques soient conservées et transmises aux utilisateurs par l'entremise d'un serveur différent de celui utilisé pour la transmission de données. L'empreinte numérique de la clé publique, qui permet d'en contrôler l'authenticité, sera conservée et transmise par une autorité crédible.
8. L'encryptage et le décryptage des données seront réalisés respective¬ment dans le PC de l'expéditeur et du destinataire. En aucun cas, ces procédures ne pourront avoir lieu au sein d'un ordinateur intermédiaire (BBS, host computer ou serveur de réseau).

2. Un Conseil provincial transmet au Conseil national un "Règlement d'utilisation d'un système de communication électronique via un système de boîte contrôle", lui soumis par la société X. en voie de constitution.

Avis du Conseil national :

En réponse à votre lettre du 14 décembre relative au système de communication éléctronique X. soumis à votre Conseil par le Docteur Y., nous avons l'avantage de vous communiquer que le Conseil national attache une importance particulière au problème de la sécurité des transmissions de documents médicaux couverts par le secret médical. Plusieurs avis ont déjà été rendus à ce propos (cf. Bull. Conseil national, n° 63, mars 1994, p. 19-20 et Bull. Conseil national, n° 65, septembre 1994, p. 22-23; vous trouverez copie de ces avis en annexe). Des recommandations relatives à l'échange entre médecins, par voie électronique, de données couvertes par le secret médical, sont actuellement en préparation au sein du Conseil national.

La description du système envisagé par X. soulève les remarques suivantes :

- s'il importe que les systèmes de mailing électroniques soient "ouverts" c-à-d accessibles à tous les utilisateurs, l'accès au système doit cependant rester limité aux médecins, personnes physiques, et exclure les associations ou sociétés qui n'ont d'ailleurs pas la possibilité de fournir une signature. Cette mesure vise à protéger notamment le secret professionnel au sein des établissements de soin;
- pour rappel, le contrat entre X. et chaque utilisateur devra être approuvé par votre Conseil;
- la description des standards utilisés est très générale. Afin de pouvoir apprécier la sécurité des systèmes proposés, il importe de connaître :
- la description et l'identification de l'algorithme d'encryptage utilisé
- l'identification du software cryptographique
- l'identification du software de communication utilisé.

***

En ce qui concerne les principes de manipulation de données confidentielles, il importe de tenir compte des considérations suivantes :

Authenticité

- élaboration de la double clé publique/secrète. Cette élaboration ne peut être réalisée en présence des délégués de X. Aucun risque ne peut être pris en ce domaine; la clé secrète est strictement personnelle et ne peut être partagée. MediRing doit donc fournir l'information nécessaire à l'usager pour lui permettre la construction de la clé sur son PC;
- X. ne peut être habilité ni à connaître ni à conserver la clé secrète. Pour parer à toute situation d'indisponibilité du propriétaire de la clé secrète, il est recommandé de confier au Conseil provincial une copie sur disquette de la clé secrète et du mot de passe qui y donne accès;
- il est suggéré que le mot ou la phrase de passe donnant accès à la copie de sécurité soit différent du mot de passe d'usage quotidien;
- la clé publique sera la seule qui pourra être transmise à X. Ce dernier doit s'engager à ne la transmettre qu'aux seuls utilisateurs médicaux de son réseau. X. doit également obtenir de ceux à qui elle confie ce "trousseau de clés", l'engagement d'en réserver strictement l'emploi à la transmission, entre médecins, de données couvertes par le secret professionnel du médecin.
  Une empreinte digitale de cette clé publique sert à permettre le contrôle de son authenticité par celui qui enverra du courrier au propriétaire de la clé. L'expéditeur devra donc avoir reçu cette empreinte digitale, soit par courrier lui adressé par le propriétaire, soit par une personne ou une autorité fiable;
- une information complémentaire est souhaitée de la part de X. quant au support informatique sur lequel la clé secrète sera conservée par le propriétaire : carte magnétique, carte à puce) ou s'agit-il d'une clé localisée sur le disque de

l'utilisateur? Dans cette dernière hypothèse, il existe un indéniable danger de rupture de la sécurité, étant donné que cette clé ne sera plus protégée que par le mot de passe;
- il y a lieu de prévoir également l'hypothèse de la transmission via réseau de la clé secrète par inadvertance du propriétaire. Des garanties doivent être données quant à l'impossibilité d'une telle manoeuvre.

Confidentialité

- codage et décodage : pas de remarque.
- rôle de X. : à préciser. Ce rôle devrait consister surtout à former les utilisateurs médecins en vue de l'usage du courrier électronique et de l'application des mesures de sécurité. Il ne peut participer au processus de création des clés car ceci introduirait plus d'insécurité que de solutions des problèmes. Il appartient à X. de proposer une administration adéquate des clés publiques et de se charger de la mise à disposition des logiciels et de tous les protocoles, lesquels doivent être conformes aux exigences du Conseil;
- central Host computer : il serait opportun de préciser les garanties de fonctionnement et/ou de dédoublement en cas de panne de cet ordinateur central. Lorsque la transmission des clés publiques se fait par le réseau, il est souhaitable, pour des raisons de sécurité, que les clés publiques soient conservées sur et transmises par serveur différent.

Fiabilité

Pas de remarque.

Disponibilité

Pas de remarque.