Recommandations relatives à la protection de la confidentialité lors de la transmission de données médicales à caractère personnel par le réseau Internet

Doc	a092004
Date de publication	17/02/2001
Origine	NR
Thèmes	Informatique Secret professionnel Internet

Le 22 avril 1995, le Conseil national émettait un avis concernant les conditions de sécurité nécessaires lors de la transmission par voie électronique de données médicales à caractère personnel identifiables (Bulletin du Conseil national n° 69, septembre 1995, p. 13). Après cinq années d'expérience, les recommandations complémentaires suivantes s'imposent.

Avis du Conseil national :

Le médecin a l'obligation légale et déontologique de respecter le secret médical. La transmission par voie électronique de données médicales à caractère personnel n'échappe pas à cette obligation.

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. Le cryptage par un système à double clé, encore dénommé système mathématique asymétrique, assure une sécurité satisfaisante.
3. Le médecin génère lui-même les clés sur son ordinateur personnel au moyen d'un logiciel obtenu auprès d'un fournisseur indépendant.
4. Afin d'authentifier la signature électronique, la clé publique devra être certifiée par un prestataire de service de certification délivrant des certificats qualifiés et indépendant du serveur de messagerie.
5. L'accès à la clé secrète est définitivement limité au seul propriétaire de celle-ci.
6. L'algorithme utilisé doit être connu et de longueur suffisante tant pour sa partie symétrique que pour la partie asymétrique.
7. Le cryptage et le décryptage des données seront réalisés respectivement dans l'ordinateur de l'expéditeur et du destinataire. En aucun cas, ces opérations ne pourront avoir lieu au sein d'un ordinateur intermédiaire consacré ou lié à la messagerie.

Avis du Conseil national du 22 avril 1995, BCN n° 69, septembre 1995, p. 13 :

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.