Santé Canada Health Canada

Bureau de la santé et l'inforoute

Initiatives internationales dans le secteur des dossiers médicaux électroniques : identification formelle et ICP

Canada

Initiatives internationales dans le secteur des dossiers médicaux électroniques : identification formelle et ICP

Bureau de la santé et l'inforoute
Santé Canada

Septembre 1998

Notre mission est d'aider les Canadiens et les Canadiennes
à maintenir et à améliorer leur état de santé.

Santé Canada

On peut se procurer des exemplaires supplémentaires auprès du :
Bureau de la santé et l'inforoute
Localisation postale 3002A2
11, avenue Holland, tour A, 2e étage
Ottawa (ON)
K1A 0K9
Tél. : 613-954-9165
Téléc. : 613-952-3226
Adresse web : http://www.hc-sc.gc.ca/ohih-bsi

Les questions et observations doivent être transmises à l'auteur Constantine Tikhonov à :
Constantine_Tikhonov@hc-sc.gc.ca.

La présente publication est également disponible sur demande sur disquette, en gros caractère, sur bande sonore ou en braille.

Also available in English under the title:
International Activities toward Electronic Health Records: Unique Identification and PKI

REMERCIEMENTS

Le Bureau de la santé et l'inforoute aimerait remercier M. Stephen Vail pour avoir révisé le document, Mme Hélène Vigeant pour avoir fait plusieurs suggestions précieuses et le Bureau de la traduction.

Table des matières

INTRODUCTION

Le processus d'adoption des dossiers médicaux électroniques dans de nombreux systèmes de soins de santé du monde doit être assorti d'un système fiable d'identification des patients, ainsi que de politiques détaillées et de lois visant à protéger la vie privée et les renseignements personnels. De nombreuses activités essentielles dépendent directement de l'identification exacte des patients, par exemple, la prestation de soins en établissement, l'administration de la santé, la gestion de l'information et les soins communautaires (1).

Le XX^{e} siècle est marqué par une révolution dans la prestation des soins de santé. Les progrès dans les domaines de la médecine et de la gestion ont donné naissance à un tout nouveau système de soins de santé. Les gens ne sont désormais plus traités seulement par un médecin. Chaque patient est maintenant pris en charge par une équipe regroupant des infirmières, de nombreux médecins consultants, des techniciens de laboratoire, des technologues de diagnostic et du personnel administratif. En outre, un patient n'est plus traité par un seul organisme. Une personne admise dans un établissement peut être transférée dans un autre pour y recevoir un traitement, puis nécessiter des soins de longue durée ou des soins à domicile. Il faut donc que les divers fournisseurs de soins puissent identifier clairement les patients et accéder à l'information concernant ces derniers à partir de plusieurs endroits de manière à assurer la continuité des soins.

LA SITUATION EN EUROPE

En Europe, les hôpitaux et les établissements de soins primaires utilisent largement les systèmes informatiques (SI) (2), surtout à des fins administratives. Les systèmes électroniques utilisés pour la conservation des dossiers médicaux ne sont pas suffisamment perfectionnés pour remplacer les dossiers conventionnels sur support papier. Les réseaux informatiques sont de plus en plus interconnectés grâce à des réseaux d'échange électronique de données. L'utilisation des dossiers médicaux électroniques dans les établissements de soins primaires et intégrés (partagés[1]) est une des caractéristiques les plus intéressantes des soins de santé en Europe.

Au cours des dix dernières années, on a observé une forte augmentation de l'utilisation des SI par les médecins de premier recours (omnipraticiens), en Europe. Ce phénomène est particulièrement observé aux Pays-Bas et au Royaume-Uni. L'augmentation du recours à la technologie dans le domaine des soins primaires dans certains pays d'Europe est illustrée à la Figure 1, tirée du rapport du *U.S. Institute of Medicine* (2).

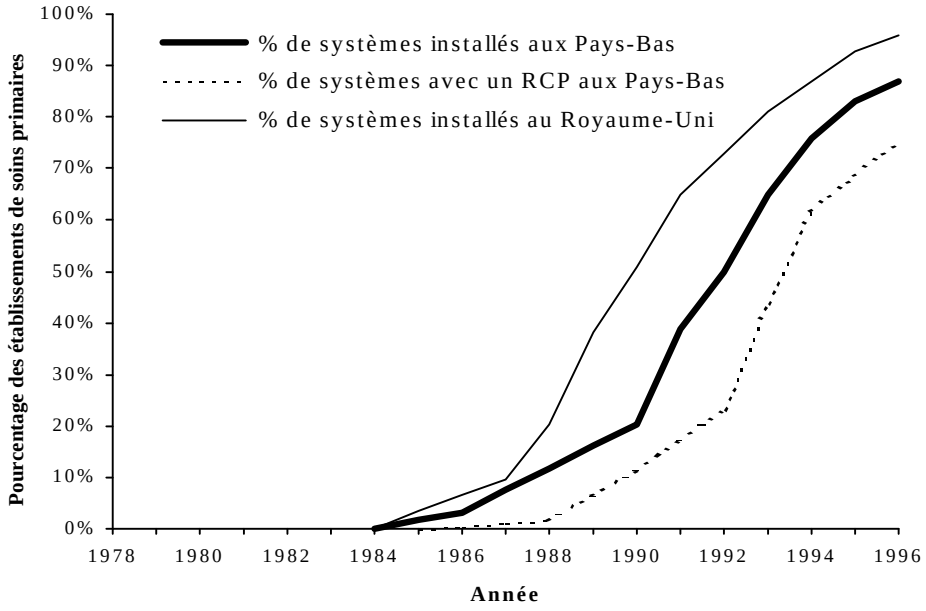

Figure 1 : Représentation temporelle de l'augmentation du nombre de systèmes installés et de dossiers médicaux informatisés dans les établissements de soins primaires aux Pay-Bas (un taux de 100 % représente 6 500 omnipraticiens), ansi qu'en Angleterre et au Pays de Galles (o un taux de 100 % représente 9 000 omnipraticiens). Les valeurs pour 1996 sont extrapolées.

[1] terme utilisé en Europe

Une telle évolution est attribuable à quatre facteurs : le rôle des omnipraticiens, la formation des médecins, la structure des soins de santé et les soins communautaires (2).

Commission européenne

Depuis 1990, la Commission européenne (CE) s'affaire à créer des systèmes d'identification des patients. La méthode utilisée est basée sur la technologie des cartes à mémoire. Plusieurs programmes et projets pilotes de R et D, ainsi qu'une initiative concertée EUROCARD ont été menés dans le cadre du troisième programme cadre de télématique appliquée à la santé (1991-1994). Ces activités avaient pour but de favoriser la convergence des initiatives nationales relatives aux cartes santé pour en arriver à des solutions communes (3).

Les activités ont été menées en collaboration avec le Comité européen de normalisation (CEN). L'analyse de l'initiative EUROCARD effectuée par dix groupes de travail a révélé que de nombreux pays d'Europe envisagent de créer des cartes à mémoire pour leur système de soins de santé. De telles cartes seraient un des éléments essentiels d'un système intégré de soins de santé (4).

La protection des renseignements personnels et la sécurité préoccupent vivement les responsables et le grand public dans les pays de l'UE (3). Si les lois visant à protéger les données varient d'un pays à l'autre, on s'entend sur certaines questions de nature générale. Par exemple, on est d'accord pour dire qu'il revient à la personne concernée de décider, de façon volontaire, d'utiliser ou non une carte contenant de l'information personnelle de nature médicale (3).

la suite de l'analyse de l'initiative EUROCARD, on suggère également d'axer la conception de l'architecture logique du contenu de la carte du patient sur une structure multidimensionnelle. Les options en matière d'accès dépendent de la nature de l'information, et les données sont habituellement réparties entre deux catégories : données administratives et données médicales. On a également reconnu la nécessité de créer une carte internationale pour les soins d'urgence. Les recommandations stratégiques découlant de l'analyse de l'initiative EUROCARD sont étudiées attentivement et validées au moyen d'activités variées liées au quatrième programme cadre (1994-1998).

Des projets de recherche et développement technologique visant une variété d'applications de dossiers médicaux électroniques ont été effectués ou sont en cours dans le cadre du quatrième programme cadre de télématique appliquée à la santé. Les projets en cours dans le domaine des soins de santé sont classés en sept groupes. La création de dossiers médicaux électroniques est un élément central du sous-programme des soins de santé.

Tous les autres projets ont trait à l'élaboration de dossiers médicaux électroniques (Figure 2).

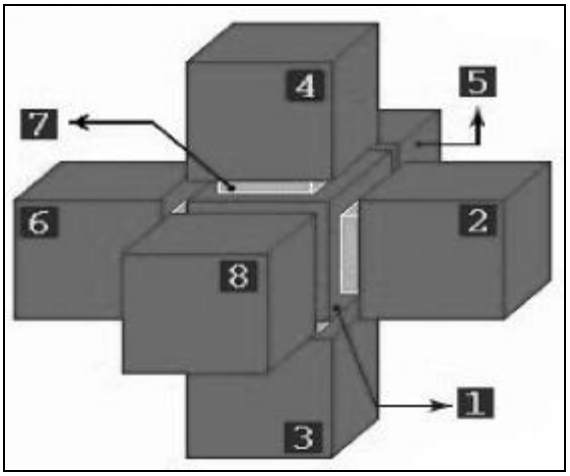

Figure 2: Rapport entre les groupes de projet dans le cadre du sous-programme de télématique appliquée à la santé : 1. Dossiers multimédia des patients; 2. Travail de collaboration assisté par la télématique pour les professionnels de la santé; 3. Systèmes des services et imagerie évoluée; 4. Plates-formes d'intégration, continuité des soins, réseaux régionaux; 5. Télédiagnostic, téléconsultation et télémédecine d'urgence; 6. Information destinée aux citoyens et aux professionnels de la santé; 7. Cohésion, diffusion et application des résultats, éducation; 8. Recherche et industrie (Adaptation du site Web de l'Observatoire européen de la télématique en santé, **www.ehto.be**)

Les projets menés par le groupe chargé des dossiers multimédia des patients sont présentés dans le tableau 1 :

Tableau 1 : Projets relatifs aux dossiers multimédia des patients dans le cadre du sous-programme de télématique appliquée à la santé

1.	**CARDLINK 2**	Dossier portable conservé par le patient et utilisé en cas d'urgence médicale
2.	**DIABCARD-3**	Communication améliorée grâce à des cartes à mémoire aux fins du traitement du diabète
3.	**EU/CEN II**	Deuxième atelier UE/CEN sur les dossiers médicaux électroniques
4.	**GALEN-IN-USE**	Architecture générale pour l'élaboration d'une encyclopédie des nomenclatures et des termes médicaux
5.	**I 4 C**	Intégration et communication pour la continuité des soins en cardiologie
6.	**I 4 C TRIPLEC**	Intégration et communication pour la continuité des soins en cardiologie
7.	**PROREC**	Stratégie de promotion du dossier médical électronique en Europe
8.	**SYNAPSES**	Serveur fédéré des dossiers médicaux
9.	**SYNEX**	Synergie sur Extranet
10.	**TELENURSE**	Applications télématiques pour les infirmières en Europe
11.	**TELENURSE ID**	Intégration et démonstration de la terminologie des soins infirmiers en Europe dans le cadre du projet de technologie de l'information
12.	**TOMELO**	Vers une alliance stratégique entre les créateurs de la terminologie médicale et des systèmes de dossiers médicaux
13	**TRUSTHEALTH**	Système fiable de télématique appliquée à la santé
14.	**WISECARE**	Système de diffusion de l'information pour le réseau européen de soins infirmiers

Trois projets portent précisément sur l'utilisation de la technologie des cartes à mémoire pour l'intégration de l'identification des patients et des dossiers médicaux électroniques.

L'objectif du projet CARDLINK 2 consiste à mettre en uvre et à faire la démonstration d'un dossier médical sur carte à mémoire conservé par le patient et utilisé en cas d'urgence médicale. Le projet est mené dans dix régions sanitaires situées dans neuf pays d'Europe (Italie, Irlande, France, Finlande, Portugal, Grèce, Pays-Bas, Allemagne et Espagne). La carte à mémoire contiendra des segments de données qui permettront d'avoir accès aux bases de données des hôpitaux et établissements de soins primaires, favorisant ainsi l'établissement de liens avec les réseaux élargis de soins de santé (5).

Le projet DIABCARD vise la mise en uvre d'un système d'information médicale basé sur la technologie des cartes à mémoire (*chip-card-based medical information system - CCMIS*) pour les soins aux malades chroniques dans les établissements de soins ambulatoires et les hôpitaux. La carte à mémoire est un dossier médical électronique portable (6). On en est maintenant à la troisième étape du projet. Le système DIABCARD peut être utilisé de façon autonome ou intégré aux systèmes d'information et aux réseaux existants. Il n'est pas nécessaire de disposer d'une infrastructure de réseau. Le système DIABCARD est utilisé conjointement avec des systèmes offerts sur le marché, soit Millennium et Diabcare®, en Autriche, en France, en Allemagne, en Grèce, en Italie et en Espagne.

Dans le cadre du projet TRUSTHEALTH, on a élaboré des caractéristiques de sécurité à clé, notamment des techniques de cryptographie et des cartes à mémoire fondées sur une identification protégée, des signatures numériques et la protection des renseignements personnels (7). Le projet TRUSTHEALTH est basé sur la technique moderne de chiffrement asymétrique à clé publique au moyen de l'algorithme RSA, qui a été adoptée comme norme par le CEN en juillet 1996. L'approche technique adoptée comprend également l'utilisation de cartes de professionnel de la santé, qui protègent les clés privées et peuvent être utilisées à partir d'un PC (7).

Le quatrième programme cadre prend fin en 1998, et l'on planifie déjà un programme pour la période 1998-2003. Selon le rapport du Conseil des besoins stratégiques (8), « *la création d'un dossier médical électronique unique et individuel utilisé dans tous les secteurs des soins de santé (prévention, diagnostic, traitement, réadaptation, soins* à *domicile), permettra d'établir une infostructure de santé reliée, intégrée et optimale. En élargissant l'accès aux soins de santé, en évitant les dédoublements coûteux et en augmentant la satisfaction des patients, le système de dossier médical électronique permettra d'atteindre l'objectif fixé. »* [Traduction]

Le rapport souligne également qu'il faut faciliter l'utilisation des dossiers médicaux électroniques sur une vaste échelle.

> « Il faut concevoir des systèmes de démonstration à grande échelle, c'est-à-dire des réseaux intégrés de soins de santé régionaux comprenant tous les éléments nécessaires, par exemple, l'architecture des dossiers des patients, l'architecture d'intégration des segments de dossiers décentralisés, et une architecture de prestation de services. Certains projets fructueux donnent à entendre qu'en favorisant l'utilisation, par les administrations publiques et particulièrement les régions, d'applications de télématique pour les transactions de base entre les hôpitaux, les omnipraticiens et les unités territoriales de soins de santé, on pourrait éliminer les différences et la résistance au changement. » (8) [Traduction]

Projet du G7

Des activités visant à relier les réseaux de santé à l'échelle mondiale et à définir les services ont été menées dans le cadre d'un projet du G7 portant sur l'universalité des applications en matière de santé. Le sous-projet 6, qui portait sur l'harmonisation internationale des cartes de données dans le domaine de la santé, visait principalement à favoriser une interopérabilité technique et fonctionnelle des cartes dans divers pays participants. On a conclu une entente d'harmonisation des plates-formes d'interopérabilité de l'Union européenne (UE) et du gestionnaire d'accès au contenu proposé par le Japon (9). On a entrepris une étude de faisabilité de « cartes G7 » destinées aux patients et aux

professionnels; par la suite, des projets pilotes ont été menés au Canada, aux États-Unis et au Japon (9).

Allemagne

La « *Versichertenkarte* », une carte d'assurance-maladie renfermant uniquement des données administratives, a été distribuée à 73 millions de cotisants à un fonds d'assurance sur une période de quinze mois close à la fin de décembre 1995. Cette carte avait une capacité de 256 octets seulement et n'était utilisée qu'à des fins administratives (10). l'heure actuelle, une douzaine de projets pilotes de cartes à mémoire pour les patients sont en cours, les plus importants se déroulant à Koblenz (« *Patientenkarte* » avec « carte A », qui contient les antécédents médicaux d'un patient et de l'information sur les médicaments prescrits (10)), à Kassel (DIABCARD) et à Berlin (3).

France

En avril 1996, le gouvernement a approuvé une stratégie triennale visant les objectifs suivants :

- distribution à chaque citoyen d'une carte à mémoire contenant des données administratives et médicales;

- accès à la carte du patient uniquement à l'aide d'une carte de professionnel de la santé;

- distribution de cartes de professionnel de la santé à tous les fournisseurs de soins de santé; ces cartes serviront aux signatures numériques, à l'accès à l'information contenue dans la carte du patient et à l'accès au réseau;

- création d'un site intranet sur les soins de santé pour communiquer les données administratives et médicales (3).

On prévoit l'utilisation de deux types de cartes pour les patients, à savoir : *Vitale 1*, une carte familiale contenant des données administratives et *Vitale 2*, une carte personnelle contenant des données administratives et des données médicales. On avait prévu la distribution de dix millions de cartes *Vitale 1* à compter du mois de novembre 1997. Cinquante millions de cartes *Vitale 2* doivent être distribuées en 1999 (11).

Le régime public d'assurance-maladie dépensera quatre milliards de francs pour les cartes à mémoire destinées aux patients. On prévoit couvrir ce co t en rationalisant le travail d'administration au sein du régime d'assurance (3).

Finlande

Le *Ministry of Trade and Industry* de Finlande et le centre de développement technologique (*Technology Development Centre – TEKES*), financent conjointement un macro-projet pilote visant à évaluer la mise en uvre restreinte d'une nouvelle carte d'identification des patients basée sur la reconnaissance des empreintes digitales. L'institut national d'assurance (*National Insurance Institution – KELA*), dirige la mise au point de nouvelles technologies et la mise en uvre du projet dans plusieurs municipalités, districts de santé et centres technologiques de Finlande (12).

La nouvelle carte permettra aux patients d'accéder, par le truchement d'Internet, à l'information médicale les concernant, tout en protégeant les renseignements personnels, grâce à la technologie de chiffrement biométrique des empreintes digitales, intégrée à la carte. On prévoit que la fiabilité des mécanismes d'authentification et de sécurité de la carte donneront lieu à une rationalisation des communications avec les professionnels de la santé, les pharmacies et d'autres intervenants. Les nouvelles cartes d'identité devraient être utilisées à partir de l'automne 1999 (12).

Royaume-Uni

Le service national de santé du Royaume-Uni (*U.K. National Health Service - NHS*), est en voie d'adopter le nouveau numéro *NHS*, qui permettra d'identifier formellement un patient. L'ancien numéro se présentait sous 22 formats différents, pouvait donner lieu à des erreurs de transcription et ne se prêtait pas à une utilisation généralisée dans des environnements informatisés (13). Le nouveau numéro comporte dix caractères présentés suivant la séquence 123 456 7899, le dernier caractère étant un caractère de validation visant à éviter les erreurs au moment de l'entrée du numéro dans les bases de données (13).

Le nouveau numéro *NHS* est considéré comme une amélioration importante en vue d'une identification plus précise, de services plus accessibles et mieux adaptés, de capacités de liaison accrues, de protection améliorée des renseignements confidentiels sur les patients et de l'amélioration de la qualité des données.

En mars 1997, on a entré le numéro *NHS* dans les principaux systèmes suivants du *NHS* (13) :

- registre central du *NHS*;
- registres des naissances et des décès;
- dossiers des patients des services de santé de la famille;
- systèmes d'administration des patients recevant des soins actifs;
- santé des enfants;
- dépistage du cancer du sein;
- contrats avec les autorités sanitaires.

Le numéro devrait être utilisé à l'échelle du système en juin 1998 (13).

Australie

En juin 1995, l'*Australian Health Ministers' Advisory Council* a créé un groupe d'étude sur la qualité des soins de santé en Australie. Dans son rapport final publié en juin 1996, le groupe a recommandé la poursuite des recherches et la mise en place de projets de démonstration. Il a également proposé que la mise en uvre d'une carte à mémoire détenue volontairement par les patients, comportant un dossier médical, fasse l'objet d'études de faisabilité et d'enquêtes pilotes (14). Le groupe d'étude a recommandé l'affectation de 575 000 $A[2] sur cinq ans à cette fin.

Nouvelle-Zélande

En 1996, le gouvernement a élaboré et publié une nouvelle « Stratégie en matière d'information santé pour l'an 2000 ». On a cerné les deux grands problèmes qui sous-tendent l'élaboration de la stratégie (15,16) :

1. la nécessité d'identifier les particuliers individuellement

[2] Un dollar australien (A) = 0,9029 dollar canadien (CAN) le 14 septembre 1998

2. la sécurité, la confidentialité des renseignements médicaux personnels et la protection de la vie privée des patients.

La stratégie a défini les éléments clés du système national de renseignements en matière de santé (15, 16) :

- Index national en matière de santé
- Fichier minimal national
- Réseau national d'information en matière de santé
- Utilisation de normes en matière de technologie, données, qualité, vie privée
- Sondage sur la santé auprès des foyers
- Base de données unique

La création d'une infrastructure nationale d'information santé en Nouvelle-Zélande repose essentiellement sur un index national en ligne qui renferme des renseignements sur chaque usager du système de santé.

Deux bases de données nationales, le *National Health Index* (*NHI*) et *le Medical Warning System* (*MWS*), constituent les volets de l'infostructure qui traitent directement les questions de sécurité et de vie privée tout en assurant aux professionnels responsables des soins aux patients un accès suffisant aux renseignements (17).

Le *NHI* est un registre basé sur la population dans lequel figurent tous les usagers du système de santé de la Nouvelle-Zélande. Chaque patient reçoit un identificateur unique qui lui est attribué au hasard. Le registre renferme les noms, pseudonymes, adresses et dates de naissance. Ces renseignements permettent l'identification formelle de chaque particulier (17).

Le *MWS* emmagasine l'information nécessaire au processus de prise de décision clinique. Il renferme des renseignements sur les allergies, les sensibilités, les antécédents médicaux et significatifs et les antécédents familiaux du particulier. Cette base de données aide les fournisseurs de soins de santé à obtenir des renseignements médicaux importants et « éventuellement salvateurs » sur un patient n'importe o en Nouvelle-Zélande (17,18).

L'identification formelle du particulier est un principe essentiel qui constitue le fondement d'un système de santé de qualité et diminue sensiblement la probabilité d'une erreur de traitement.

La *Privacy Act* (1993) a imposé des restrictions en ce qui concerne l'usage des identificateurs et le *NHI* est conforme à toutes les directives. La *Privacy Act* prévient l'utilisation des données du *NHI* pour des motifs non liés à la prestation des services de santé et des renseignements qui se rapportent à ces services. Les données du *NHI* ne peuvent être reliées aux bases de données des autres secteurs de l'économie ni aux bases de données utilisées à d'autres fins. En vertu de la loi, quelques particuliers autres que les fournisseurs de soins de santé peuvent être autorisés à avoir accès aux données du *NHI*, tandis que les données du *MWS* sont accessibles uniquement aux professionnels de la santé appelés à traiter une personne (18).

États-Unis d'Amérique

La *Health Insurance Portability and Accountability Act* (1996) énonçait un processus visant l'adoption de normes nationales relatives aux données médicales et à la protection des renseignements médicaux aux États-Unis.

Le tableau 2 présente le cadre réglementaire actuel.

Tableau 2 : Normes américaines relatives aux données médicales : cadre législatif (19)

La loi exige que le *Secretary of Health and Human Services* (*HHS*) adopte des normes à l'appui de l'échange électronique d'une variété de transactions administratives et financières en matière de santé. Les régimes d'assurance-maladie, les bases de données médicales, et les fournisseurs de soins de santé qui veulent effectuer les transactions précisées par voie électronique doivent se conformer aux normes dans les deux années suivant leur adoption. Les petits régimes d'assurance-maladie disposent de trois ans. Voici quelques-unes des normes :

1. Certaines transactions et données uniformes concernant les demandes de règlement et les renseignements équivalents obtenus lors des rencontres, les pièces jointes aux demandes de règlement, les avis de paiement des soins médicaux et d'envois d'argent, l'adhésion et la fin de l'adhésion aux régimes d'assurance-maladie, l'admissibilité aux régimes d'assurance-maladie, les paiements de primes d'assurance-maladie, le premier rapport de blessure, le statut des demandes de règlement, l'homologation et l'autorisation des références et la coordination des prestations.
2. **Identificateurs uniques pour les particuliers, les employeurs, les régimes d'assurance-maladie et les fournisseurs de soins de santé à l'usage du système de santé.** [L'accent est ajouté.]
3. Ensembles de codes et de systèmes de classification relatifs aux données des transactions précisées.
4. **Normes de sécurité relatives aux renseignements médicaux.** [L'accent est ajouté.]
5. **Normes relatives aux procédés de transmission électronique et à la validation des signatures en ce qui a trait aux transactions précisées.** [L'accent est ajouté.]

   Les mesures visant à protéger la vie privée et la confidentialité des renseignements médicaux jouent également un rôle prépondérant dans la loi. Le *Secretary* est tenu d'adopter des normes de sécurité pour sauvegarder l'information médicale pendant la transmission et le stockage dans les systèmes informatiques. Ces normes visent à assurer l'intégrité de l'information et à empêcher les usages non autorisés et les divulgations. En outre, la loi exige que le *Secretary* présente des recommandations détaillées au Congrès relativement à la protection des renseignements médicaux portant sur des particuliers identifiables. Ces recommandations ont été présentées au Congrès le 11 septembre 1997. Si le Congrès n'adopte pas une loi visant la confidentialité des dossiers médicaux d'ici le 21 ao t 1999, la loi exige que le *Secretary* émette des règlements visant à protéger la confidentialité des renseignements médicaux des particuliers identifiables transmis dans le cadre de transactions standard. Ces règlements doivent être finalisés d'ici le 21 février 2000.

Au cours des deux dernières années, des organismes du *Department of Health and Human Services (DHHS)* américain ont mené d'importantes recherches sur les identificateurs uniques destinés aux usagers et aux fournisseurs des services de santé. Ces travaux ont été effectués dans le cadre d'une simplification de l'administration. Le projet de règlement concernant l'identificateur du fournisseur national (*National Provider Identifier – NPI*) a été publié en mai 1998 (20) et a fait l'objet de consultations publiques jusqu'au 6 juillet 1998.

Selon le projet de règlement, le *NPI* est un identificateur alphanumérique de huit chiffres. Le huitième chiffre sert à désigner les *NPI* non valides ou erronés. On s'attend à ce que

l'utilisation du *NPI* améliore les programmes *Medicare* et *Medicaid* et les autres programmes de santé administrés par le gouvernement fédéral, ainsi que l'efficacité et l'efficience globales du système de santé américain.

Le *DHHS* entend publier un avis d'intention (*Notice of Intent – NOI*) qui favorisera les discussions sur les contre-propositions relatives à un identificateur personnel et aux questions connexes. Il a également préparé un livre blanc sur l'identificateur unique personnel en matière de santé afin de fournir les renseignements nécessaires en prévision des audiences publiques du *National Committee on Vital and Health Statistics* (*NCVHS*) (19). Le livre blanc fournit un aperçu détaillé des avantages que procurent aux particuliers les identificateurs personnels uniques, ainsi qu'une analyse des propositions mises d'avant en ce qui concerne l'identificateur personnel unique (19) :

1. ASTM[3] *Sample Universal Healthcare Identifier* (*UHID*)

2. Numéro de sécurité sociale (*Social Security Number - SSN*), y compris la proposition du *(Computer-based Patient Record Institute - CPRI)*[4]

3. Identificateurs biométriques

4. Service d'annuaire

5. Propriétés individuelles immuables

6. Système d'identification du patient fondé sur le numéro de dossier médicalexistant et le préfixe du praticien

7. Système cryptographique à clé publique-à clé privée

Le *NCVHS* a recommandé que le *DHHS* n'approuve pas de norme visant un identificateur unique pour les particuliers avant que la loi sur la protection de la vie privée n'ait été adoptée. Il a notamment mentionné « *…qu'il serait malavisé et prématuré de procéder au choix et* à *la mise en* œ*uvre d'un tel identificateur avant qu'une loi assurant la*

[3] *American Society for Testing and Materials*

[4] Le *Computer-based Patient Record Institute* a publié un document de travail en 1993, recommandant que le numéro de sécurité sociale, modifié et émis selon un nouveau processus, devienne l'identificateur universel en matière de santé pour les particuliers. En 1996, le *CPRI* a publié le document intitulé *Action Plan for Implementing a Unique Health Identifier*, v. 1.0, qui explique la proposition en détail (20).

confidentialité des renseignements médicaux des particuliers identifiables et la protection de la vie privée des particuliers n'ait été adoptée ». (21) [Traduction]

RÉCENTES INITIATIVES VISANT LE DOSSIER MÉDICAL ÉLECTRONIQUE

Royaume-Uni

Le *NHS Information Management Group* (*IMG*) publiera sous peu une nouvelle stratégie en matière de G.I.T. pour le *NHS*. Préparée l'an dernier, cette stratégie est étroitement liée au programme global du gouvernement visant à moderniser le *NHS* et à miser sur les possibilités des technologies de l'information pour améliorer la qualité, l'accessibilité et la responsabilité au sein du système de santé. L'objectif fondamental de la stratégie sera de créer des dossiers patients électroniques pour tous les citoyens, lesquels seront accessibles à tous les fournisseurs du système national de santé (22). La stratégie intégrera plusieurs systèmes déjà élaborés : un réseau privé national basé sur les protocoles TCP/IP (*NHSNet*), un service d'écrasement par le truchement de la passerelle X.400 permettant le traitement des données financières dans l'ensemble du système national de santé, un identificateur unique pour chaque résident du Royaume-Uni, un dictionnaire de codes cliniques standard et des systèmes gérant les dossiers patients et la rédaction d'ordonnances installés dans 90 p. 100 des cabinets des médecins généralistes (22). Grâce à la stratégie, on disposera d'un dossier patient unique intégré permanent, qui sera à la disposition de tous les organismes du système national de santé 24 heures par jour.

Prenant la parole lors de la conférence organisée dans le cadre du 50^{e} anniversaire du *NHS*, le très honorable Tony Blair a déclaré qu'il appuyait entièrement le transfert de renseignements par voie électronique.

Le groupe chargé des dossiers patients électroniques de l'*IMG* a récemment lancé un disque CD-ROM expliquant les avantages des dossiers patients électroniques pour les fournisseurs de soins de santé, les patients et le public en général et faisant la promotion de ce nouvel outil.

États-Unis d'Amérique

Les activités visant à intégrer le dossier médical électronique (dossier patient informatisé, dossier médical électronique – *Electronic Health Record - EHR*) à l'infostructure de la santé aux États-Unis sont hâtées par l'existence d'immenses organismes de maîtrise des dépenses de santé, qui sont de plus en plus intégrés verticalement (p. ex. Kaiser Permanente, Columbia/HCA).

Les systèmes de dossiers médicaux électroniques les plus perfectionnés aux États-Unis ont été mis en uvre dans plusieurs centres médicaux universitaires et hôpitaux d'enseignement affiliés aux universités, ainsi qu'au *Department of Veterans Affairs* et au *Department of Defense* (*DOD*) (23).

Le projet gouvernemental de dossier patient informatisé *(Government Computer-based Patient Record – G-CPR*) du *DOD* américain est le projet le plus remarquable de 1998. Un cadre relatif au *G-CPR* sera élaboré en vue de générer et de protéger les dossiers médicaux permanents des membres des forces armées. Le cadre sera ensuite élargi à la population civile. Le projet est le résultat d'un partenariat entre le *Department of Defense*, le *Department of Veterans Affairs*, l'*Indian Health Service* et le *Louisiana State University Medical Centre*. Les plans stratégiques de mise en uvre du cadre sont en place.

En avril 1998, le *DOD* a annoncé la signature de sept contrats séparés en vertu de son programme de gestion de l'information médicale/d'intégration, de conception, d'élaboration, d'exploitation et de maintenance des systèmes II (*D/SIDDOMS II*), conçu pour fournir des services de gestion de l'information et de technologie de l'information à l'appui du système de santé militaire (*Military Health System – MHS*) du *DOD*. Litton PRC a obtenu le contrat d'intégrateur de cadre primaire. On affectera 20 millions de dollars au premier volet de l'intégration du cadre et 200 millions de dollars par an au cours des cinq années suivantes (communication personnelle).

La valeur globale des sept contrats pourrait atteindre 2,5 milliards de dollars, si toutes les options sont levées au cours de la période quinquennale. Le système de santé militaire du *DOD* est l'un des plus vastes et des plus compliqués de la planète. Il appuie 120 hôpitaux militaires et 500 cliniques. Le *MHS* dessert plus de 1,7 million de membres en service actif et 6,2 millions d'anciens membres retraités, les membres de leurs familles et leurs bénéficiaires (24).

INFRASTRUCTURE DE CLÉ PUBLIQUE (ICP)

Un papier blanc sur l'infrastructure de clé publique du gouvernement du Canada (25) affirme que l'ICP assure la sécurité des transactions électroniques et du partage de renseignements de nature délicate par l'entremise de clés et de composantes de chiffrement. Par suite de la mise en uvre de l'ICP, les fonctions de sécurité suivantes seront assurées : confidentialité, contrôle d'accès, intégrité, authentification et non-répudiation. Le Centre de la sécurité des télécommunications a défini l'ICP comme étant une combinaison des composantes suivantes :

- Autorité de certification
- Logithèque des certificats
- Système de révocation des certificats
- Système de secours et de récupération des clés
- Soutien à la non-répudiation
- Mise à jour automatique des clés
- Gestion des historiques des clés
- Certification croisée
- Horodateur
- Interaction régulière et fiable du logiciel client avec les éléments précités.

États-Unis d'Amérique

En mai 1996, l'*Office of Management and Budget* (*OMB*) a publié un livre blanc intitulé *Enabling Privacy, Commerce, Security, and Public Safety in the Global Information Infrastructure*[5]. Le livre blanc affirmait que « le gouvernement et l'industrie doivent collaborer à la création d'une infrastructure de gestion sécuritaire et de produits auxiliaires

[5] Peut être consulté en ligne à l'adresse **http://www.cdt.org/crypto/clipper_III/clipper_III_draft.html**

qui intègrent une cryptographie robuste sans nuire à la sécurité nationale ni à la sécurité du public. » [*Traduction]*

Depuis l'automne 1996, l'administration fédérale américaine a adopté une politique qui favorise la croissance et l'usage de systèmes de gestion des clés avec récupération intégrée des clés. L'administration fédérale entend avoir recours à ce genre de solution, même lorsqu'elle communique avec des sociétés et des particuliers. Des projets sont en cours en vue de permettre au marché d'élaborer des solutions.

Plusieurs organismes participent activement à l'élaboration de la technologie ICP aux États-Unis (26). En voici quelques-uns :

- La commission américaine *Federal Government Information Technology Services* (*GITS*) a mis sur pied un comité directeur fédéral ICP chargé d'offrir des conseils aux organismes fédéraux au sujet de la mise en uvre d'une ICP fédérale (**http://gits-sec.treas.gov/**). Le comité directeur fédéral ICP a approuvé presque 50 projets pilotes associés à l'ICP au sein du gouvernement fédéral.

- Le *National Institute of Standards and Technology* (*NIST*) dirige l'élaboration d'une ICP fédérale qui appuie les signatures numérisées et autres services de sécurité publics basés sur les clés (**http://csrc.nist.gov/pki/**).

- En plus de participer au comité directeur fédéral ICP, le *NIST* se penche sur plusieurs questions importantes liées à la mise en uvre de l'ICP (p. ex., l'élaboration d'une norme minimale d'interopérabilité pour les composantes de l'ICP, la préparation d'un point de repère de mise en uvre et de la mise en uvre initiale d'une autorité de certification (*Certification Authority – CA*) centrale pour l'ICP fédérale).

- L'*OpenGroup's Security Program Group* élabore une architecture d'ICP (**http://www.rdg.opengroup.org/public/tech/security/pki**). Il collabore présentement avec des experts d'autres organismes (p. ex., *IETF*, CommerceNet, projets financés par la Commission européenne) en vue de définir une architecture d'ICP commune.

Union européenne

Le programme *RTD* de la Commission européenne élabore actuellement une infrastructure de clé qui sera l'une des composantes d'une infrastructure de tierces parties de confiance. La gestion des clés publiques est un aspect essentiel de l'infrastructure de clé et, par conséquent, elle est souvent utilisée en association avec l'ICP. Pour obtenir un aperçu détaillé des normes et spécifications auxquelles les organismes de l'Union européenne ont recours lors de la conception de l'infrastructure ICP, consulter le document *Security Guide*, publié sur Internet par l'*European Open Information Interchange* (**http://www2.echo.lu/oii/en/secguide.html**).

On procède à l'élaboration des composantes sécuritaires des dossiers médicaux électroniques et des activités relatives à l'inscription par l'entremise d'un éventail de projets pilotes et de projets de démonstration au sein de la section de la télématique appliquée à la santé du programme de télématique appliquée (p. ex., *TRUSTHEALTH*, *TRUSTHEALTH 2*, *ISHTAR*).

Le projet *ISHTAR*[6] (*Implementing Secure Healthcare Telematics Applications in Europe*), est l'une des initiatives les plus importantes menées par l'Union européenne dans le secteur de la transmission protégée des renseignements médicaux. Le projet de 36 mois a débuté en février 1996 (27). Douze pays participent aux activités menées dans le cadre du projet *ISHTAR* (le Royaume-Uni, la Grèce, la Belgique, les Pays-Bas, l'Allemagne, l'Irlande, le Portugal, la Finlande, l'Italie, la France, la Suisse et la République tchèque). Un des prédécesseurs du projet *ISHTAR* fut *SEISMED* (*Secure Environment for Information Systems in Medicine*), projet mené entre 1992 et 1995 dans le cadre du programme *AIM* (*Advanced Informatics in Medicine*). Les résultats, qui ont été publiés dans un guide en trois volumes, servent présentement de référence pour l'élaboration des normes de sécurité en matière de santé, présentement effectuée par le Comité Européen de Normalisation (CEN) comité technique 251 (informatique médicale) (28). Les objectifs du projet *ISHTAR* figurent dans le tableau 3.

[6] Renseignements tirés du document *Compendium of Health Telematics Projects* 94-98 (27)

Tableau 3 : Objectifs du projet ISHTAR

- Créer un groupe de spécialistes des aspects juridique, médical et technique de la protection des données dans le secteur de la santé. Les membres du groupe assumeront un rôle consultatif et agiront à titre de consultants auprès de la Commission et des autres projets du quatrième programme cadre de télématique appliquée à la santé ayant des besoins en matière de sécurité. Le groupe établira également des liens avec tous les forums nationaux, européens et internationaux en matière de sécurité.

- Fournir des mécanismes relatifs à la mise en uvre, à la validation et au maintien des normes de protection des données médicales et élaborer un mode de déclaration d'incident dans le secteur de la santé.

- Améliorer les normes de sécurité présentement en vigueur dans le secteur de la santé en réglant les aspects techniques de la protection des renseignements médicaux à l'aide de la télématique et démontrer leur utilité et leur efficacité.

- Sensibiliser le public et le personnel de la santé aux questions liées à la protection des données médicales en présentant des séminaires et en diffusant les résultats obtenus à l'échelle internationale.

- Cerner et analyser les problèmes légaux et sociaux soulevés par la télémédecine et le réseautage dans le secteur de la santé.

Suède

La Suède procède à l'élaboration d'une politique nationale en matière de cryptographie. En première étape, on a préparé un rapport sur la politique cryptographique (29), qui a été présenté par le *Swedish Cabinet Office Reference Group for Cryptographic Issues* au ministre du Commerce international en octobre 1997. Selon ce rapport, aucune restriction ne vise l'importation, l'élaboration et l'usage de la cryptographie en Suède. Cependant, à l'été 1997, l'utilisation du PGP dans la gestion des clés était la seule occurrence de l'infrastructure de clé publique en Suède (29).

Nouvelle-Zélande

La Nouvelle-Zélande a abordé la question de la confidentialité des renseignements en deux étapes. En juillet 1993, la *Privacy Act* a assuré la protection juridique de tous les renseignements personnels, y compris l'information médicale. Elle s'applique aux secteurs public et privé, et vise tous les formats d'information. Cette loi a permis l'élaboration de « codes d'usage » destinés à des organismes et à des activités précises. Elle a également instauré des mécanismes de contrôle pour les registres publics (16).

Conformément au règlement afférent à la *Privacy Act*, le Commissaire à la vie privée a émis un « code d'usage » s'adressant tout particulièrement à la protection de la vie privée en ce qui concerne les renseignements médicaux personnels. Le « *Health Information Privacy Code 1994* » s'applique à tous les organismes de secteur des soins de santé et énonce des règlements relatifs à (16) :

- la collecte de renseignements personnels;
- l'emmagasinage et la sécurité;
- l'accès et la correction;
- l'utilisation et la divulgation;
- la mise à jour et la disposition;
- des identificateurs uniques.

Aux termes de la *Privacy Act* (1993), le respect de la vie privée relève des cadres de direction. Les dirigeants des organismes du secteur de la santé sont tenus d'élaborer et de mettre en place des plans de gestion « appropriés en matière de vie privée ». Chaque organisme de la santé est tenu d'assurer la présence d'un ou plusieurs responsables du respect de la vie privée au sein de l'organisme (16).

Australie

En Australie, un groupe de travail représentant le gouvernement, l'industrie et les consommateurs a présenté une proposition relative à un cadre d'authentification des clés publiques (*Public Key Authentication Framework - PKAF*).[7] Le système prévu est volontaire, non assujetti à un permis gouvernemental et traiterait uniquement de l'authentification. Le *PKAF* sert d'autorité de certification, et non de tiers de confiance. Les clés seront générées conformément au cadre, afin d'assurer l'intégrité et la sécurité du système. Cependant, le *PKAF* ne conservera pas la clé et aucun accès gouvernemental au

[7] *Standards Australia* a distribué une ébauche du document *Australian Standard on Strategies for the Implementation of a Public Key Authentication Framework in Australia* le 1er avril 1996, en vue de recueillir des commentaires, et l'a publié en tant que *Miscellaneous Publication* (MP75) le 5 novembre 1996 (renseignements tirés du rapport Walsh (30)).

système n'est prévu. La proposition a été élaborée sous les auspices de *Standards Australia*, conformément aux normes techniques et de gestion. Selon le rapport Walsh (30), l'adoption du cadre nécessitera un amendement à l'*Evidence Act* ou à l'*Acts Interpretation Act*, afin que la signature numérique ait la même autorité et le même effet qu'une signature écrite à la main. La confidentialité et la sécurité des renseignements recueillis par la *Health Insurance Commission* et le *Department of Health and Family Services* fédéral sont également régis par les directives en matière de vie privée des programmes *Medicare* et *Pharmaceutical Benefits* (31).

Japon

Le groupe de travail *Certification Authority Working Group* (*WG8*) du *Electronic Commerce Promotion Council of Japan* (*ECOM*) a amorcé la définition des politiques d'ICP en 1996. Le groupe de travail a publié un rapport d'étape en avril 1997 (32). Ce document jette le fondement de l'exploitation d'une autorité de certification, autorisée à délivrer des certificats numériques. L'ICP est définie comme étant une « infrastructure robuste destinée à assurer la sécurité des transactions commerciales électroniques et autres systèmes d'information, et la fiabilité du système de communication. » (32) [*Traduction]*

RÉFÉRENCES

1. Appavu S. *Analysis of Unique Patient Identifier Options*, rapport final, U.S. Department of Health and Human Services, 24 novembre 1994.

2. Van Bemmel J.H., van Ginneken A.M., van der Lei J. « A Progress Report on Computer-Based Patient Records in Europe », dans Dick R.S., Steen E.B., Detmer D.E. (éd.), *The Computer-Based Patients Record: An Essential Technology for Health Care*, éd. rév., IOM, National Academy Press, Washington, 1997 : 21–43. Adresse Internet : **http://www.nap.edu/readingroom/**

3. Doare H. *Data Cards in Healthcare*. Allocution présentée à la session consacrée à la télématique de la santé dans le cadre de la conférence EUROCHINATEL, avril 1997.

4. EUROCARD Action Overview, Commission européenne DG XIII, rapport final. 3rd Framework Programme Telematics Systems for Health Care (AIM) 1991–1994. Adresse Internet : **http://www.ehto.be/aim/volume2/eurocards.html**

5. CARDLINK 2 Project Overview, EHTO. Internet : **http://www.ehto.be/ht_projects/7groups.html#I**

6. Site Web du projet DIABCARD : **http://www-mi.gsf.de/diabcard/index.html**

7. Site Web du projet TRUSTHEALTH : **http://www.ehto.be/projects/trusthealth/**

8. Commission européenne DG XIII. *Telematics Application Programme: Needs & Options for Future Research in the Field of Telematics for Healthcare.* Rapport du Strategic Requirements Board, 1997. Adresse Internet : **http://www2.echo.lu/telematics/health/health.html**

9. G-7 Global Healthcare Applications Project, 6e rapport d'étape, décembre 1996. Internet : **http://www.ispo.cec.be/g7/projects/g7heal6.html**

10. Schaefer O.P. *Evolution of Health Care Cards & Networks in EUROPE*, Central Research Institute of Ambulatory Health Care in Germany, ZI. Présentation en PowerPoint à CardTech SecurTech 1997. Adresse Internet : **http://www.va.gov/card/card9705/Orlando1.ppt**

11. Fraval Y., ministère de la Santé, France. *Health Cards in France.* Présentation en PowerPoint à CardTech SecurTech 1997. Adresse Internet : **http://www.va.gov/card/card9705/YF.ppt**

12. « Health services by fingerprint recognition be piloted in Finland ». Aamulehti online, *ETHOS News Digest.* Adresse Internet : **http://www.tagish.co.uk/ethos/news/lit1/fa0e.htm**

13. NHS Executive. *The NHS Number: Putting the NHS Number to Work.* Compte-rendu du *NHS* et du programme de service de repérage. Adresse Internet : **http://www1c.btwebworld.com/imt4nhs/general/nhsno/work.htm**

14. *The Final Report of the Taskforce on Quality in Australian Health Care*, juin 1996. Adresse Internet : **http://www.health.gov.au/pubs/hlthcare/toc.htm**

15. Johnston J.A. *Implementing the Health Information Strategy for New Zealand.* MEDINFO 95 Proceedings, IMIA, 1995 : 1608-1611

16. *Health Information Strategy for New Zealand: A Joint Venture between the Area Health Boards and the Department of Health*, octobre 1991. Adresse Internet : **http://www.health.govt.nz/HIS2000/index.html**

17. New Zealand Health Information Service Publications, *National Health Index and Medical Warning System.* Adresse Internet : **http://www.nzhis.govt.nz/publications/NHI-MWS.html**

18. New Zealand Health Information Service Publications, *Health Information Privacy and Confidentiality*, décembre 1995. Adresse Internet : **http://www.nzhis.govt.nz/publications/Privacy.html**

19. *Unique Health Identifier for Individuals*. Livre blanc, DHHS américain. Adresse Internet : **http://aspe.os.dhhs.gov/admnsimp/nprm/noiwp1.htm**

20. *National Standard Health Care Provider Identifier*, Proposed Rule, HCFA, DHHS, Federal Register/vol. 63, n° 88 : p. 25320 à 25357. Adresse Internet : **http://aspe.os.dhhs.gov/admnsimp/nprm/npilist.htm**

21. NCVHS Recommendation to the Secretary of the U.S. Department of Health and Human Services. Adresse Internet : **http://aspe.os.dhhs.gov/ncvhs/uhid.htm**

22. Mitchell P. « UK's NHS Unveils IT Strategy », *Healthcare Informatics Magazine*, juillet 1998. **http://www.healthcareinformatics.com/issues/1998/07_98/inter.htm**

23. Tang P.C., Hammond W.E. « A Progress Report on Computer-Based Patient Records in the United States », dans Dick R.S., Steen E.B., Detmer D.E. (éd.), *The Computer-Based Patients Record: An Essential Technology for Health Care*, éd. rév., IOM, National Academy Press, Washington, 1997 : 1-20. Adresse Internet : **http://www.nap.edu/readingroom/**

24. Pietrucha, Bill. « Department of Defense to Modernize Military Health System », communiqué de presse du DOD, *Newsbytes*, Washington, DC, 23 avril 1998 (NB)

25. *The Government of Canada Public Key Infrastructure*, livre blanc, Centre de la sécurité des télécommunications, février 1998.

26. « Public Key Infrastructure Technology », *ITL Bulletin*, juillet 1997. Adresse Internet : **http://www.nist.gov/itl/lab/bulletns/july97bull.htm**

27. *Compendium of Health Telematics Projects 94-98* (ébauche), ISHTAR. Adresse Internet : **http://www.ehto.be/ht_projects/html/dynamic/77.html**

28. *Data Security for Health Care*, IOS Press. Adresse Internet : **http://www.iospress.nl/html/node168.html#SECTION00031211700000000000000**

29. *Cryptography Policy: Possible Courses of Action for Sweden*. Rapport émanant du Swedish Cabinet Office Reference Group for Cryptographic Issues, octobre 1997. Ministry for Foreign Affairs Department for Strategic Export Control, SE-103 39. Stockholm, Suède

30. Walsh G. *Review of Policy Relating to Encryption Technologies.* Rapport préparé pour le Department of the Attorney General. Security Division, 1997. Adresse Internet : **http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm**

31. *Privacy and the Public Sector.* Site Web du commissaire à la vie privée de l'Australie : **http://www.privacy.gov.au/public/index.html**

32. *Certification Authority Guidelines* (Alpha), Certification Authority Working Group, Electronic Commerce Promotion Council of Japan (ECOM); 10e étage, Édifice Time 24, 2-45 Aomi, Koto-ku, Tokyo 135-75, Japon. Tél. : 03-5531-0065, téléc. : 03-5531-0068, courrier électronique : yonekura@ecom.or.jp ou kakuma@ecom.or.jp Adresse Internet : **http://www.ecom.or.jp**