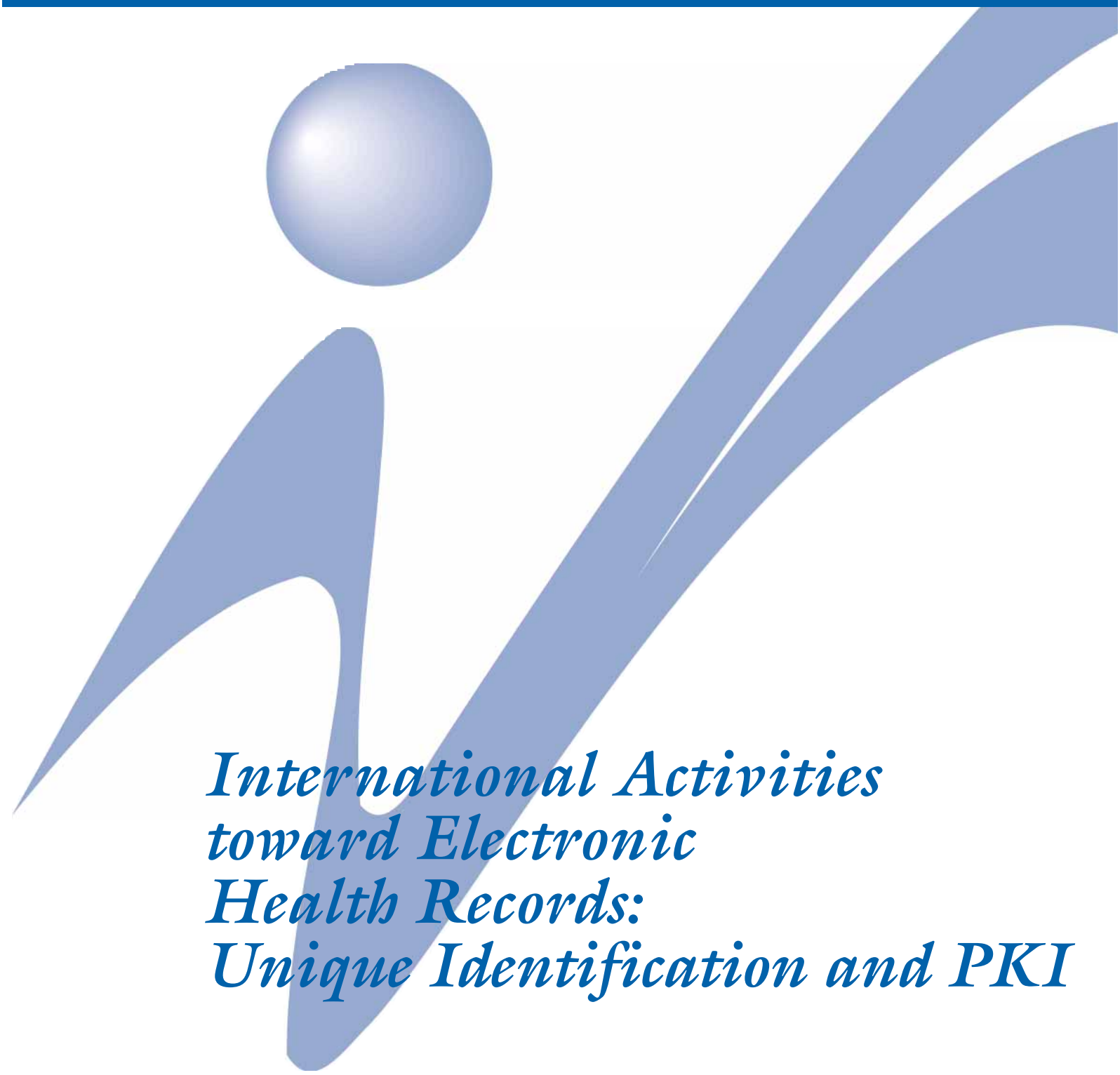
Health Canada Santé Canada

*Office of Health and the Information Highway*



# *International Activities toward Electronic Health Records: Unique Identification and PKI*

Canada

# International Activities toward Electronic Health Records: Unique Identification and PKI

Office of Health and the Information Highway
Health Canada

**September 1998**

Our mission is to help the people of Canada
maintain and improve their health.

*Health Canada*

Additional copies are available from:
Office of Health and the Information Highway
Postal Locator 3002A2
11 Holland Avenue - Tower A - Second Floor
Ottawa ON
K1A 0K9
telephone: (613) 954-9165
fax: (613) 952-3226
website address: http://www.hc-sc.gc.ca/ohih-bsi

Questions and comments should be addressed to the author Constantine Tikhonov at:
Constantine_Tikhonov@hc-sc.gc.ca.

This publication can be made available in/on computer diskette, large print, audio-cassette or braille upon request.

Également disponible en français sous le titre :
Initiatives internationales dans le secteur des dossiers médicaux électroniques : identification formelle et ICP

## ACKNOWLEDGMENTS

The Office of Health and the Information Highway would like to acknowledge the assistance of Mr. Stephen Vail for reviewing this paper, Ms. Judith Whitehead for English editing, and Ms. Hélène Vigeant for providing communications support.

## Table of Contents

## INTRODUCTION

A reliable system for patient identification, coupled with comprehensive policies and/or legislative acts protecting privacy of individuals and security of personally identifiable information, is a necessary component of the electronic health record implementation process in many health care delivery systems around the world. Many vital activities directly depend on correct identification of patients, such as the delivery of institutional care, health administration, information management and community care activities (1).

The twentieth century is characterized by a revolution in provision of health care services. Advances in medical science and management have created an entirely new system of health care. People are not cared for by a single physician any longer. Instead, it is a collective process that includes nurses, many consulting physicians, laboratory technicians, diagnostic technologists and administrative staff. Moreover, a patient is no longer treated by one organization. A person can be admitted to one facility, transferred to another for treatment, and then require extended or home care. Therefore, it is necessary to uniquely identify patients across multiple providers and be able to access their information from multiple locations in order to support continuity of care.

## EUROPEAN ACTIVITIES

The use of computer information systems (IS) is widely spread in European hospitals and primary care (2). The majority of institutional IS is oriented toward administration. The development of electronic patient record systems has not reached the level where they can substitute for paper-based file systems. IS networks are increasingly interconnected by electronic data interchange. The use of electronic health records in primary care and integrated (shared[1]) care is one of the most interesting characteristics of health care in European countries.

In the last ten years, there has been an impressive increase in the rate of IS adoption by European primary care physicians (GPs). This process has been particularly notable in the Netherlands and the United Kingdom. The growth in the use of technology in primary care of some European countries is presented in Figure 1 from the U.S. Institute of Medicine report (2).

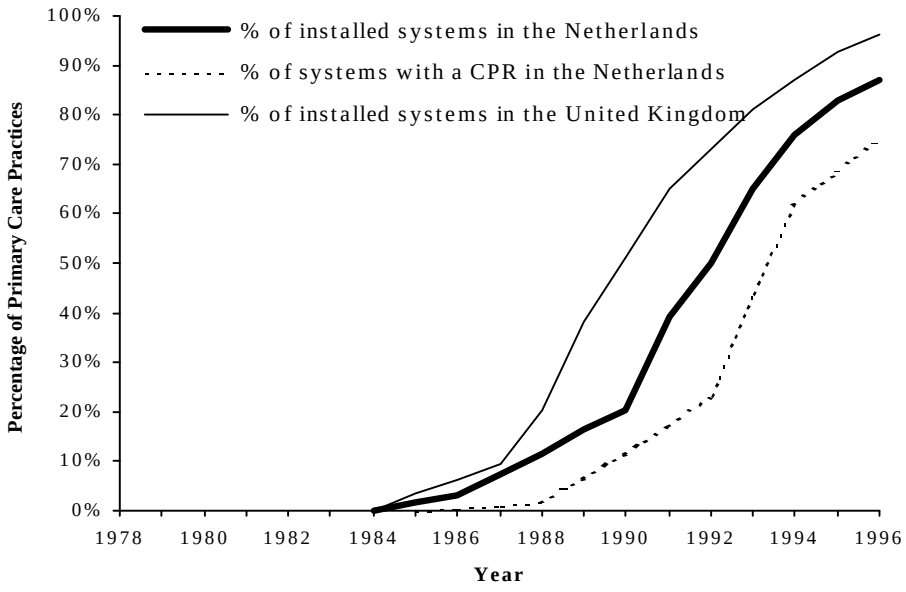



**Figure 1:** Growth of installed information systems and computer-based patient records in primary care in The Netherlands (100% represents 6,500 general practitioners [GPs]) and England and Wales (where 100% represents 9,000 GPs) as a function of time. The values for 1996 are extrapolations.

[1] European term

Such substantial progress is attributed to four factors: the role of GPs, physician training, the structure of health care and population-based care (2).

**European Commission**

Since 1990, the European Commission (EC) has been very active in designing systems for unique patient identification. The European approach is centred on smart card technology. Several R&D projects and pilot activities and a concerted EUROCARDS action have been conducted within the Third Framework of the Telematics for Healthcare Program (1991-94). The purpose of these activities was to foster the convergence of national initiatives on health cards toward common or interoperable solutions (3).

These activities were conducted in cooperation with the European Committee for Standardization (CEN). The analysis conducted by ten working groups of the EUROCARDS action showed that many European countries are considering the development of smart cards for their health care system. Such a card was not seen as a stand-alone element, but as a key component of an integrated health information system (4).

The issues of confidentiality and security are of major concern for EU authorities and the general public (3). Despite the difference in data protection legislation in place in European countries, some broad issues were agreed upon. For example, there is a consensus that the decision to use a card containing personal medical information should remain with the person on a voluntary basis (3).

The EUROCARDS action also suggested implementing a layered approach for designing the logical architecture of patient data card content. The access options depend on the sensitivity of information and are generally structured into two categories: administrative data and medical data. The need to create an international emergency card was also identified. The EUROCARDS strategic recommendations are being extensively explored and validated by different activities of the Fourth Framework Programme (1994-98).

A range of electronic health record (EHR) applications represents a core of research and technological development projects that have been completed or are being guided through the Fourth Framework Telematics Applications Programme. All ongoing projects in health care are organized into seven groups. Development of EHRs is a centrepiece of the health care sub-program. All other projects are associated with the development of EHR (Figure 2).

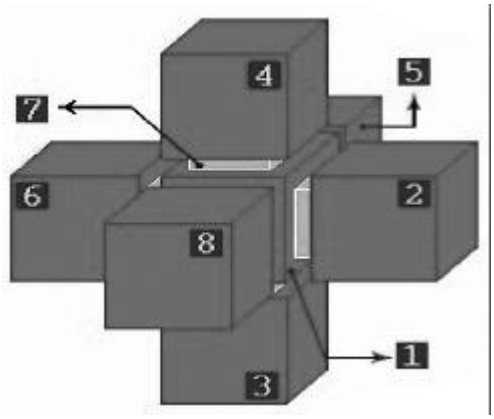



**Figure 2: Relationship between the project groups within the Telematics for Healthcare sub-programme:**
1. Multimedia Patients Records; 2. Telematics Assisted Cooperative Work for Healthcare Professionals; 3. Departmental Systems & Advanced Imaging; 4. Integration Platforms, Continuity of Care, Regional Networks; 5. Telediagnosis, Teleconsultation & Emergency Telemedicine; 6. Information for Citizens & Health Sector Professionals; 7. Cohesion, Dissemination & Exploitation of Results, Education; 8. Research & Industry (Adopted from the WWW site of the European Health Telematics Observatory, **www.ehto.be**)

The projects conducted within the Multimedia Patient Records group are presented in Table 1:

*Table 1: Multimedia Patients Records Projects of the Telematics for Healthcare Sub-programme*

| | | |
|---|---|---|
| 1. | **CARDLINK 2** | A patient-held portable record for use in cases of medical emergency |
| 2. | **DIABCARD-3** | Improved communication in diabetes care based on chip cards |
| 3. | **EU/CEN II** | The second EU/CEN workshop on the electronic health care record |
| 4. | **GALEN-IN-USE** | Generalized architecture for language encyclopedia and nomenclatures in medicine |
| 5. | **I 4 C** | Integration and communication for the continuity of cardiac care |
| 6. | **I 4 C TRIPLEC** | Integration and communication for the continuity of cardiac care |
| 7. | **PROREC** | Promotion strategy for the European electronic health care record |
| 8. | **SYNAPSES** | Federated health care record server |
| 9. | **SYNEX** | Synergy on Extranet |
| 10. | **TELENURSE** | Telematic applications for nurses in Europe |
| 11. | **TELENURSE ID** | Integration and demonstration of European nursing terminology in Information Technology Project |
| 12. | **TOMELO** | Toward a strategic alliance between developers of medical terminology and health care record systems |
| 13 | **TRUSTHEALTH** | Trustworthy health telematics |
| 14. | **WISECARE** | Workflow information systems for European nursing care |

Three projects are specifically addressing the use of smart card technology for integrating patient identification and the electronic health record system.

The objective of the CARDLINK 2 project is to implement and demonstrate a patient-held smart card medical record for particular application in cases of medical emergency. The project sites are located in ten health regions in nine European countries (Italy, Ireland, France, Finland, Portugal, Greece, the Netherlands, Germany, Spain). The smart card will contain a series of data segments to enable access to hospital and primary care databases, thus establishing linkages with the wider health care networks (5).

The DIABCARD project aims at implementing and testing a chip card-based (smart card) medical information system (CCMIS) for chronic diseases in ambulatory and hospital care. The smart card serves as a portable electronic health record (6). The project is now in its third phase. DIABCARD can be used as a stand-alone system or it can be integrated into existing information systems and networking environments. An existing network infrastructure is not necessary. The DIABCARD system is being implemented on the basis of commercially available systems, Millennium and Diabcare®, in Austria, France, Germany, Greece, Italy and Spain.

The TRUSTHEALTH project developed key security specifications, including cryptographic techniques and smart cards for secure identification, digital signatures and confidentiality (7). TRUSTHEALTH is based on modern, asymmetric public key encryption with the RSA-algorithm, which was approved as a CEN standard in July 1996. The technical approach of TRUSTHEALTH further includes the use of Healthcare Professional Cards that protect the private keys and allow portability to any PC working place (7).

The Fourth Framework Programme ends in 1998, and a planning process is under way for 1998 to 2003. According to the report prepared by the Strategic Requirements Board (8), *enabling the existence of single, individual electronic health care record (EHR) covering all care settings (prevention, diagnosis, treatment, rehabilitation, home care) will result in connected, integrated, and optimized health infostructure. By increasing access to health care, avoiding costly duplication and increasing patient satisfaction the electronic health record system will fulfill its goal.*

The report also stressed that there is a need to enable deployment of the EHR on a broad scale.

> "There is a need for large-scale demonstrators, i.e. integrated regional healthcare networks demonstrating all required elements, such as patient record architecture, integration architecture of decentralised patient record segments, and a service provision architecture. A few success cases suggest that getting public administrations, and particularly the regions to employ telematic applications in the basic transactions between hospitals, GPs and territorial HC units, could be the triggering mechanism to overcome differences and resistance to change" (8).

## G7 Project

A number of activities directed at linking health networks on a global level and at identification of services was conducted within the context of a G-7 Global Healthcare Application Project. The main emphasis of the work conducted by sub-project 6, "International harmonization of data cards in healthcare," was placed on enabling technical and functional interoperability of the cards in different participating countries. An agreement has been reached on convergence between the European Union (EU) interoperability platform and the Japanese proposal for Content Access Manager (9). A feasibility study of "G7-Cards" for patients and professionals was undertaken, and was followed by pilots in Canada, United States and Japan (9).

## Germany

The "Versichertenkarte," a health insurance card containing only administrative data, was issued to 73 million members of insurance funds for 15 months until the end of December 1995. It only had a 256-byte capacity and was strictly an administrative card (10). There are about 12 patient smart card pilot projects currently under way, the most important ones being conducted in Koblenz ("Patientenkarte" with "A-Card," storing patient history and drug prescription information (10)), Kassel (DIABCARD) and Berlin (3).

## France

In April 1996, the government approved a three-year strategy aimed at the:

- distribution of the smart card, containing administrative and medical information, to each citizen;
- access to the patient card only by using a health professional card;
- distribution of health professional cards to all health care providers to be used for digital signature, access to patient card information and to access the network; and

- creation of the health care intranet to communicate administrative and medical information (3).

Two types of patient cards are planned: Vitale 1 is a family card with administrative data and Vitale 2 is a personal card with administrative and medical information. It was planned that 10 million Vitale 1 cards were to have been issued starting in November 1997. Fifty million Vitale 2 cards are supposed to be issued in 1999 (11).

The cost of the patient smart card for the national health insurance organization is four billion FF. The cost is expected to be covered by simplification of the administrative work within the insurance system (3).

**Finland**

The Finnish Ministry of Trade and Industry and the Technology Development Centre (TEKES) are funding a macro trial project to evaluate limited implementation of the entirely new patient identification card with fingerprint recognition. The National Insurance Institution (KELA) is leading the development of new technologies and the rollout of the project in several Finnish municipalities, health care districts and technology centers (12).

The purpose of new card is to enable patients to access information on their health condition via the Internet, while protecting their privacy with fingerprint-based biometric encryption technology embedded in the card. It is expected that the reliability of authentication and security mechanisms provided by the card will result in streamlined communication with health professionals, pharmacies and others. The new ID cards are expected to be ready for implementation by the fall of 1999 (12).

**United Kingdom**

The U.K. National Health Service (NHS) is in the process of full implementation of the new NHS number, which will enable unique and unambiguous identification of a patient. The old number had 22 different formats, was liable to transcription errors and was not suitable for extensive use within computerized environments (13). The new number has ten digits that are displayed as 123 456 7899, with the last digit being a validation digit designed to prevent errors when entering the number in electronic databases (13).

The new NHS number is perceived as an important advance toward improved accuracy of identification, enhanced accessibility and responsiveness of services, improved linkage capability, increased patient confidentiality and improved data quality.

By March 1997, the NHS number was successfully installed on the following key systems of the NHS (13):

- NHS Central register
- Registrars of Births and Deaths
- family health service patient registers
- acute patient administration systems
- child health
- breast screening
- health authority contracting.

The full use of the number was planned for June 1998 (13).

**Australia**

In June 1995, the Australian Health Ministers' Advisory Council established a Task Force on Quality in Australian Health Care. Its final report was released in June 1996. Among recommendations to provide additional research and conduct demonstration projects, the Task Force suggested that "the introduction of a voluntary patient held 'smart card' for health records be the subject of feasibility and pilot studies"(14). The Task Force suggested allocating AUS$575,000[2] over five years for this purpose.

**New Zealand**

In 1996, the government developed and released a new "Health Information Strategy for the Year 2000." The first two issues recognized as being major in the development of the strategy were (15,16):

1. the need to identify individuals uniquely; and
2. the security, confidentiality and privacy of personal health information.

The strategy identified the key elements of the national health information system

[2] 1 Australian Dollar (AUD) = 0.9029 Canadian Dollar (CAD) September 14, 1998

(15, 16):

- National Health Index
- National Minimum Data Set
- National Health Information Network
- Use of standards for technology, data, quality, privacy
- Household Health Survey
- Single Clearing House

The cornerstone in building the national health information infrastructure in New Zealand is an on-line National Health Index, which contains information on each health care user.

Two national databases, the National Health Index (NHI) and the Medical Warning System (MWS), are the centre of the infostructure that directly addresses the issues of security and privacy, while providing sufficient accessibility to information for professionals responsible for patient care (17).

The NHI is a population-based register of all users of health care in New Zealand. Every patient is assigned a unique identifier on a random basis. The register maintains records of names, aliases, addresses and date of birth. This enables positive and unique identification of an individual (17).

The MWS stores information that is important for a clinical decision-making process. It maintains records on an individual's allergies, sensitivities, significant and relevant medical and family history. This database assists health care providers in obtaining important and "potentially life-saving medical information" about a specific patient anywhere in New Zealand (17,18).

The positive and unique identification of an individual is a critical principle that lays out a foundation for quality health care and significantly lessens the probability of potentially dangerous mistreatment**.**

The Privacy Act of 1993 placed restrictions on the use of unique identifiers, and the NHI conforms to all guidelines. The Privacy Act safeguards NHI numbers from being used for any purpose other than in conjunction with the provision of health care services, and of information relating to those services. NHI numbers cannot be related to databases from other sectors of economy, or databases used for different purposes. According to the law, a few individuals other than health care providers may be allowed to access NHI data, and the access to MWS is restricted solely to health professionals in the context of care for the person (18).

### United States of America

The Health Insurance Portability and Accountability Act of 1996 outlined a process to adopt national health data standards and health information privacy in the United States.

Details of the current regulatory environment are outlined in Table 2.

***Table 2: The U.S. Health Care Data Standards: Legislative Environment (19)***

The law requires that the Secretary of Health and Human Services (HHS) adopt standards to support the electronic exchange of a variety of administrative and financial health care transactions. All health plans, health care clearinghouses, and those health care providers who elect to conduct the specified transactions electronically are required to comply with the standards within 2 years of their adoption, except that small health plans are required to comply within 3 years. Among these standards are:

1. Certain uniform transactions and data elements for health claims and equivalent encounter information, claims attachments, health care payment and remittance advice, health plan enrollment and disenrollment, health plan eligibility, health plan premium payments, first report of injury, health claim status, referral certification and authorization, and for coordination of benefits.
2. **Unique identifiers for individuals, employers, health plans, and health care providers for use in the health care system.** [emphasis added]
3. Code sets and classification systems for the data elements of the transactions identified.
4. **Security standards for health information.** [emphasis added]
5. **Standards for procedures for the electronic transmission and authentication of signatures with respect to the transactions identified.** [emphasis added]

Privacy and confidentiality protections for health information play a prominent role in the law as well. The Secretary is required to adopt security standards to safeguard health information, during transmission and while stored in health information systems, to ensure the integrity of the information, and to protect against unauthorized uses and disclosures. Further, the law requires the Secretary to make detailed recommendations to the Congress for protection of individually identifiable health information. These recommendations were delivered to the Congress on September 11, 1997. If the Congress does not enact legislation for health record privacy by August 21, 1999, the law requires the Secretary to issue regulations to protect the privacy of individually identifiable health information transmitted in standard transactions. These regulations must be finalized by February 21, 2000.

In the last two years, agencies of the U.S. Department of Health and Human Services (DHHS) have been conducting extensive research concerning unique health identifiers for individuals and providers. This work has been conducted in the framework of Administrative Simplification. The proposed rule concerning the National Provider Identifier (NPI) was published in May 1998 (20) and until July 6, 1998 was a subject for public comments.

According to the proposed rule, the NPI is an eight-number alphanumeric identifier. The eighth digit is used to identify invalid or erroneous NPIs. The use of NPIs is expected to improve Medicare and Medicaid programs and other federally managed health programs, as well as the overall efficiency and effectiveness of the U.S. health care system.

DHHS is planning to publish a Notice of Intent (NOI) to facilitate discussion about the alternatives for a health identifier for individuals and related issues. DHHS has also prepared a White Paper on the Unique Health Identifier for Individuals to make information available before the public hearings by the National Committee on Vital and Health Statistics (NCVHS) (19). The White Paper provides a clear overview of the benefits of the unique identifiers for individuals and analysis of available proposals for the unique identifier (19):

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

2. Social Security Number (SSN), including the proposal of the Computer-based Patient Record Institute (CPRI)[4]

3. Biometric Identifiers

4. Directory Service

5. Personal Immutable Properties

6. Patient Identification System based on existing Medical Record Number and practitioner Prefix

[3] The American Society for Testing and Materials

[4] The Computer-based Patient Record Institute published a working paper in 1993, recommending that the SSN, with alterations in the number and the process for issuing it be ratified as a universal health identifier for individuals. In 1996, the CPRI published an *Action Plan for Implementing a Unique Health Identifier*, v. 1.0, which elaborated on the details of the proposal (20).

### 7. Public Key-Private Key Cryptography Method

The NCVHS recommended that the DHHS not adopt a standard for a unique identifier for individuals until the privacy legislation has been adopted. It was stated that *"…it would be unwise and premature to proceed to select and implement such an identifier in the absence of legislation to assure the confidentiality of individually identifiable health information and to preserve an individual's right to privacy."* (21)

## LATEST ACTIVITIES TOWARD AN ELECTRONIC HEALTH RECORD

### United Kingdom

The NHS Information Management Group (IMG) is about to release a new IM&T strategy for the NHS. This strategy has been prepared during the last year, and is closely related to the overall government's agenda to modernize NHS and to capitalize on IT's potential to improve quality, access and accountability within the health care system. The fundamental goal of the strategy will be creating EPRs for all citizens, nationally accessible by any NHS health care provider (22). The upcoming strategy will incorporate several already developed systems: a nation-wide private TCP/IP-based network (NHSNet), an X.400-based clearing service for processing financial information across the NHS, a unique health identifier for every U.K. citizen, a standard clinical coding dictionary, and systems for patient documentation and prescription writing, installed in 90 percent of general practitioners' offices (22). The strategy is expected to result in a single, integrated lifetime patient record, available 24 hours a day to every NHS organization.

Speaking at the NHS 50th Anniversary Conference, the Prime Minister, the Right Honourable Tony Blair, expressed full support for the use of electronic transfer of information.

The EPR group of the IMG has recently released a multimedia CD-ROM explaining the benefits and promoting the use of electronic patient records to health care providers, patients and the general population.

### United States of America

Activities related to the development of the EHR (computer-based patient record, electronic medical record) as a component of the U.S. health infostucture are accelerated by the existence of the very large, increasingly vertically integrated, managed care organizations (e.g., Kaiser Permanente, Columbia/HCA).

The most advanced EHR systems implemented in the United States can be found in several academic medical centres and teaching hospitals affiliated with universities, as well as in the Department of Veteran Affairs and the Department of Defense (DOD) (23).

One of the most remarkable initiatives of 1998 is the Government Computer-based Patient Record (G-CPR) Initiative of the U.S. DOD. A G-CPR framework is to be developed as a means of providing and protecting worldwide life-long medical records of Armed Forces personnel. In the future, the framework will be extended to the civilian population. The

initiative is a result of partnership between the DOD, Department of Veteran Affairs, the Indian Health Service and Louisiana State University Medical Centre. The strategic plans for the framework implementation are in place.

In April 1998, DOD announced seven separate contracts under its Defense Medical Information Management/Systems Integration, Design, Development, Operations, Maintenance Services II (D/SIDDOMS II) program, designed to provide IM and IT services in support of the DOD Military Health System (MHS). Litton PRC was contracted as a primary "framework integrator." The initial task of the framework integration will receive $20 million and be followed with $200 million per year over five years (personal communication).

The seven contracts have a combined potential value of $2.5 billion if all options are exercised over the five-year period. DOD's MHS is one of the world's largest, most intricate health care systems, supporting 120 military hospitals and 500 clinics. MHS delivers services to more than 1.7 million active duty service members and to 6.2 million military retirees, dependants and beneficiaries (24).

## PUBLIC KEY INFRASTRUCTURE (PKI)

A white paper on the Government of Canada Public Key Infrastructure (25) states that PKI enables secure electronic transactions and the exchange of sensitive information through the use of cryptographic keys and certificates. As a result of implementing PKI, the following security functions will be achieved: confidentiality, access control, integrity, authentication and non-repudiation. The Communication Security Establishment defined PKI as a combination of the following components:

- Certification Authority
- Certificate Repository
- Certificate Revocation System
- Key Backup and Recovery System
- Support for Non-Repudiation
- Automatic Key Update
- Management of Key Histories
- Cross-certification
- Timestamping
- Client-side software interacting with all of the above in a consistent and trustworthy manner

### United States of America

In May 1996, the Office of Management and Budget (OMB) released a White Paper entitled *Enabling Privacy, Commerce, Security, and Public Safety in the Global Information Infrastructure*.[5] This paper stated that "government and industry must work together to create a security management infrastructure and attendant products that incorporate robust cryptography without undermining national security and public safety."

[5] Available on-line at: **http://www.cdt.org/crypto/clipper_III/clipper_III_draft.html**

Since the fall of 1996, the U.S. federal administration adopted a policy that promotes the growth and usage of key management systems with built-in key recovery. The federal administration intends to use such solutions, even in its communication with companies and individuals. Initiatives are being taken to enable the market to produce solutions. Several organizations are actively involved in the development of the PKI technology in the United States (26). Some of them are:

- The U.S. Federal Government Information Technology Services (GITS) board has established a Federal PKI Steering Committee to provide guidance to federal agencies regarding the establishment of a federal PKI (**http://gits-sec.treas.gov/**). The Federal PKI Steering Committee approved nearly 50 PKI-related pilots throughout the federal government.

- The National Institute of Standards and Technology (NIST) has a leadership role in the development of a ederal PKI that supports digital signatures and other public key-enabled security services (**http://csrc.nist.gov/pki/**).

- In addition to participating in the Federal PKI Steering Committee, NIST is working on several key issues enabling implementation of PKI (e.g., developing a Minimum Interoperability Specification for PKI Components, developing a reference implementation and the initial implementation of a root Certification Authority (CA) for the federal PKI).

- The OpenGroup's Security Program Group is developing architecture for PKI (**http://www.rdg.opengroup.org/public/tech/security/pki)**. It is currently working with experts in other organizations (e.g. IETF, CommerceNet, European Commission funded projects) to define a common architecture for a PKI.

**European Union**

A key infrastructure is being developed by the European Commission RTD Programme as a component of a Trusted Third Parties Infrastructure. An essential aspect of a key infrastructure is the management of public keys and, therefore, it is often used synonymously with PKI. For a detailed overview of standards and specifications used by EU organizations in the design of the PKI infrastructure, please refer to the Security Guide, published on the Internet by the European Open Information Interchange (**http://www2.echo.lu/oii/en/secguide.html**).

Development of the security components of EHR and registration activities is being addressed through a range of coordinated pilot and demonstration projects within the Telematics for Healthcare section of the Telematics Application Programme (e.g., TRUSTHEALTH, TRUSTHEALTH 2, ISHTAR).

The ISHTAR[6] (Implementing Secure Healthcare Telematics Applications in Europe) project is one of the largest initiatives conducted by the EC in the field of secure communication of health information. The 36-month project started in February 1996 (27). ISHTAR activities are conducted in 12 participating countries (United Kingdom, Greece, Belgium, the Netherlands, Germany, Ireland, Portugal, Finland, Italy, France, Switzerland and Czech Republic). One of the predecessors of ISHTAR was the SEISMED (Secure Environment for Information Systems in Medicine) project conducted between 1992 and 1995 as part of the AIM (Advanced Informatics in Medicine) Programme. The results were published in a three-volume handbook and have been passed for reference in the current development of health care security standards by the Comité Européen de Normalisation (CEN) Technical Committee 251 (Medical Informatics) (28). The goals of the ISHTAR project are presented in Table 3.

[6] Information is compiled according to the *Compendium of Health Telematics Projects* 94-98 (27)

**Table 3: ISHTAR Project Goals**

- Creating a group of experts on legal, medical and technical aspects of data protection in health care. This group will act as an advisory panel and "consultants" to both the Commission and to other Fourth Framework Health Telematics Projects facing security needs. The group will also interface with all the relevant national, European and International security forums.
- Providing the means for implementing, validating and maintaining existing guidelines on health data protection and providing a health care incident reporting scheme.
- Enhancing existing security guidelines for health care by addressing the technical aspects of health data protection within the context of telematics applications and demonstrating their usefulness and practicality.
- Increasing the awareness of both the public and health care personnel on issues related to health data protection through awareness seminars and worldwide dissemination of its results.
- Identifying and analyzing the legal and societal issues raised by telemedicine and networking in health care.

### Sweden

Sweden is in the process of developing a national cryptographic policy. One of the first steps in this process was a compilation of a report on cryptography policy (29), presented by the Swedish Cabinet Office Reference Group for Cryptographic Issues to the Minister of International Trade in October 1997. According to this report, there are no restrictions on the import, production and use of cryptographic technology in Sweden. However, as of summer 1997, "the use of PGP for key management is probably the only note worthy occurrence of a so-called Public Key Infrastructure in Sweden" (29).

### New Zealand

New Zealand has addressed the information privacy issue in two steps. On July 1993, the Privacy Act provided legal protection regarding all personal information, including health information. It applies in the public and private sectors and to any information formats. This legislation enabled "codes of practice" to be formulated encompassing specific organizations and activities. It also placed controls on the administration of public registers (16).

In consonance with the regulation of the Privacy Act, the Privacy Commissioner issued a "code of practice" specifically addressing privacy protection in regard to personal health information. The "Health Information Privacy Code 1994" applies to all health care sector organizations and formulates rules applicable to (16):

- collecting personal information;
- storage and security;
- access and correction;
- use and disclosure;
- updating and disposal; and
- unique identifiers.

According to the Privacy Act 1993, privacy is the responsibility of top-level management. Managers of health sector organizations are required to formulate and implement "appropriate privacy management" plans. Each health agency is required to make sure that it has one or more privacy officers within the organization (16).

**Australia**

In Australia, a working group representing government, industry and consumers produced a public key authentication framework (PKAF) proposal.[7] The system is planned as voluntary, not subject to government license and would deal only with authentication. The PKAF function is that of a certifying authority, not a trusted third party. Keys would have to be generated in accordance with the framework to ensure integrity and security. However, PKAF will not retain the key and no government access to the system is proposed. The proposal was developed under the auspices of Standards Australia and conforms to both management and technical standards. According to the Walsh Report (30), its adoption will require amendment to the Evidence Act or the Acts Interpretation Act to provide for a digital signature to have the same force and effect as a hand-written signature. The confidentiality and security of health information collected by the Health

[7] A draft Australian Standard on Strategies for the Implementation of a Public Key Authentication Framework in Australia was issued for comment by Standards Australia on 1 April 1996 and was released as a Miscellaneous Publication (MP75) on 5 November 1996 (cited from the Walsh Report (30)).

Insurance Commission and the federal Department of Health and Family Services are also regulated by the Medicare and Pharmaceutical Benefits Programs privacy guidelines (31).

**Japan**

The Certification Authority Working Group (WG8) of the Electronic Commerce Promotion Council of Japan (ECOM) started working on defining PKI policies in 1996. The working group published its interim report in April 1997 (32). This document lays the foundation for the operation of a Certification Authority, which is authorized to issue digital certificates. The PKI is defined as a "robust infrastructure for ensuring the security of commercial electronic transactions and other information systems, and the reliability of the communication system." (32)

## REFERENCES


1. Appavu S. *Analysis of Unique Patient Identifier Options*, Final Report, U.S. Department of Health and Human Services, November 24, 1994.

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

3. Doare H. *Data Cards in Healthcare*. Speech at the EUROCHINATEL Conference's session on health telematics, April 1997.

4. EUROCARD Action Overview, European Commission DG XIII, Final Report. 3rd Framework Programme Telematics Systems for Health Care (AIM) 1991–1994. 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. DIABCARD Project Web Site: **http://www-mi.gsf.de/diabcard/index.html**

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

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

9. G-7 Global Healthcare Applications Project, 6th Progress Report, December 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. PowerPoint presentation at CardTech SecurTech 1997. Internet: **http://www.va.gov/card/card9705/Orlando1.ppt**

11. Fraval Y., Ministry of Health, France. *Health Cards in France.* PowerPoint presentation at CardTech SecurTech 1997. Internet: **http://www.va.gov/card/card9705/YF.ppt**

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

13. NHS Executive. *The NHS Number: Putting the NHS Number to Work.* Briefing Report of the NHS Number and Tracing Service Programme. Internet: **http://www1c.btwebworld.com/imt4nhs/general/nhsno/work.htm**

14. *The Final Report of the Taskforce on Quality in Australian Health Care*, June 1996. 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*, October 1991. Internet: **http://www.health.govt.nz/HIS2000/index.htm**

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

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

19. *Unique Health Identifier for Individuals*. A White Paper, The U.S. DHHS. 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, No. 88: pp. 25320–25357. 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. Internet: **http://aspe.os.dhhs.gov/ncvhs/uhid.htm**

22. Mitchell P. "UK's NHS Unveils IT Strategy," *Healthcare Informatics Magazine*, July 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," in Dick R.S., Steen E.B., Detmer D.E. (eds.), *The Computer-Based Patients Record: An Essential Technology for Health Care*, rev. ed., IOM, National Academy Press, Washington, 1997: 1-20. Internet: **http://www.nap.edu/readingroom/**

24. Pietrucha, Bill. "Department of Defense to Modernize Military Health System," DOD press release, *Newsbytes*, Washington, DC, 1998 April 23 (NB)

25. *The Government of Canada Public Key Infrastructure*, White Paper, Communication Security Establishment, February 1998.

26. "Public Key Infrastructure Technology," *ITL Bulletin*, July 1997. Internet: **http://www.nist.gov/itl/lab/bulletns/july97bull.htm**

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

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

29. *Cryptography Policy: Possible Courses of Action for Sweden*. A report from the Swedish Cabinet Office Reference Group for Cryptographic Issues, October 1997. Ministry for Foreign Affairs Department for Strategic Export Control, SE-103 39. Stockholm, Sweden

30. Walsh G. *Review of Policy Relating to Encryption Technologies.* Report for the Attorney General's Department. Security Division, 1997. Internet: **http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm**

31. Privacy and the Public Sector. Australian Privacy Commissioner's Web Site: **http://www.privacy.gov.au/public/index.html**

32. Certification Authority Guidelines (Alpha), Certification Authority Working Group, Electronic Commerce Promotion Council of Japan (ECOM); Floor 10, Time 24 Building, 2-45 Aomi, Koto-ku, Tokyo 135-75, Japan Tel: 03-5531-0065 Fax: 03-5531-0068 E-mail: yonekura@ecom.or.jp or kakuma@ecom.or.jp. Internet: **http://www.ecom.or.jp**