International Journal of Medical Informatics (2004) **73**, 259—266

ELSEVIER

International Journal of Medical Informatics

www.intl.elsevierhealth.com/journals/ijmi

Access and authorisation in a Glocal e-Health Policy context

Richard E. Scott*, **Penny Jennett**, **Maryann Yeo**

Global e-Health Research and Training Program, Health Telematics Unit, G204 Health Sciences Centre, Faculty of Medicine, University of Calgary, 3330 Hospital Drive NW, Calgary, Alberta, Canada T2N 4N1

KEYWORDS
Telemedicine;
e-Health;
Electronic health record (EHR);
Health Policy;
Access;
Authorisation

Summary Challenges to the development of appropriate yet adaptable policy and tools for security of the individual patient electronic health record (EHR) are proving to be significant. Compounding this is the unique capability of e-health to transgress all existing geo-political and other barriers. Initiatives to develop and advance policy, standards, and tools in relation to EHR access control and authorisation management must address this capability. Currently policy development initiatives take place largely in an isolated manner. This jeopardises the potential of e-health because decisions made in one jurisdiction might hamper, even prevent, an e-health opportunity in another.

This paper places access and authorisation issues in an overall policy context through describing current Canadian initiatives. The National Initiative for Telehealth (NIFTE) Guidelines project is developing a framework of national guidelines for telehealth. The Policy and Peer Permission (PPP) project is developing a unique tool that provides persistent protection of data. The new corporate body 'Infoway' is developing a pan-Canadian electronic health record solution. Finally, the Glocal e-Health Policy initiative is developing a tool with which to identify and describe the inter-relationships of e-health issues amongst policy levels, themes, and actors.

1. Introduction

Issues of access and authorisation in relation to health information are as old as medicine itself. The original medical policy statement, the Hippocratic Oath, speaks of: ''Whatever, in connection with my professional service [*i.e. authorisation*], or not in connection with it, I see or hear [*i.e. access*], in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret''. Even in 400 BC, there appears to have been the need for discretionary powers, with the individual physician judging that ''which ought not to be spoken of abroad''. In current times differences include the wide extent to which medical information can be disseminated (*access*), the number and diversity of individuals who, potentially, desire to gain access (*authorisation*), and the decreasing acceptance of individual discretionary and professional judgement (*policy*).

Developing policy that balances the need for access (and concomitantly authorisation) with the needs and rights of the citizen in their various health roles, is a significant challenge. This is especially so when inter-jurisdictional considerations are introduced. There is a need to examine what steps must be taken to accommodate e-health within the existing administrative and policy infrastructure and, only where necessary, develop new policy and guidelines. There is also a need to

*Corresponding author. Tel.: +1-403-2207017; fax: +1-403-2708025.
E-mail address: rescott@ucalgary.ca (R.E. Scott).

1386-5056/$ — see front matter © 2003 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.ijmedinf.2003.11.020

recognise the value of early inter-jurisdictional collaboration in developing principles, guidelines, and complementary policy that will be expected to facilitate, not hamper, inter-jurisdictional exchange and access to patient information.

Recent Canadian initiatives take steps to develop clear tools and strategies to address access and authorisation (and other policy issues), to implement a pan-Canadian EHR, and to recognise the broader policy context and ultimate global value of e-health. These initiatives include the National Initiative for Telehealth (NIFTE) Guidelines [1], The Policy and Peer Permission (PPP) System Development program [2], the Canada Health Infoway Incorporated (CHII) [3], and the 'glocal' e-Health Policy initiative.

2. Terminology

Access has been found to have several descriptions, and is considered here to be 'having the ability to input or retrieve information, when necessary' [4].

Authorisation is the granting of rights, which includes the granting of access based on access rights [5].

Jurisdiction is a generic descriptive term used here for any identifiable 'unit' that possesses some autonomy in providing or presiding over healthcare services and activity within a defined sphere of authority (e.g. hospital, health region, administrative region, country, international agency). *Intra-jurisdictional* describes activity within a single jurisdiction (e.g. single hospital or single health region), and *inter-jurisdictional* refers to activity that takes place between one or more jurisdictions. The term 'cross-jurisdictional' is discouraged since it implies bi-directional interaction and crossing of a single barrier. e-Health has the potential to cross many barriers (and different types) in a single activity, which is implied through use of the term inter-jurisdictional.

e-Health Policy has been defined as 'a set of statements, directives, regulations, laws, and judicial interpretations that direct and manage the life cycle of e-health' [6].

Global e-health has been used for some time as a conceptual term. But the convergence of three recent developments—globalisation [7], global health [8,9], and the network age [10]—has allowed global e-health to emerge as a new reality that has been defined [11].

'*Glocal*' is a term that has appeared recently in the global health literature, and is a blend of 'global' and 'local' [12]. Its value lies in providing a succinct reminder of a simple but profound insight—in our networked world; what happens locally has global impact, and what happens globally has local impact.

3. National Initiative for Telehealth (NIFTE) Guidelines

NIFTE is a multi-stakeholder, interdisciplinary, and national project, that is nearing completion. Its primary outcome will be the development of a framework of national guidelines for telehealth for use by several stakeholders [1]. These include regulated health professionals (in developing their specific standards), telehealth provider organisations (as a benchmark for service provision), and the Canadian Council on Health Services Accreditation (CCHSA, in developing accreditation standards).

An environmental scan, consisting of a literature review, a mail survey, and interviews with key informants in the field of telehealth, assessed the current status of policy and standards related to telehealth practice in Canada. A second component developed a sustainable network of telehealth stakeholders and created a Stakeholder Database that will facilitate ongoing integrated, multi-sectoral collaboration. The database lists contact information for organisations, associations, government and individuals with expertise and interest in telehealth and national guidelines, and now lists over 300 individuals and groups.

The primary value of this initiative will stem from its final component; development of the NIFTE Framework of Guidelines. The environmental scan, complemented by key informant data, will formulate a package to provide guidance in four policy areas related to telehealth: organisational context, human resources, technology and equipment, and clinical standards and outcomes.

4. Policy and Peer Permission (PPP)

The efficient and secure management of patients' EHR is a key issue in the development of a workable, e-health system. More important is security of this information 'in transit'. Canada's PPP system, also nearing completion, will automate the authoring and interpretation of policy for granting access (authorization) to EHR's. Unique aspects of PPP are: its ability to provide persistent security automatically in a practicable manner, protecting sensitive data no matter where it goes; and its policy based system that relies on *rules* rather than specific statements to generate its permissions,

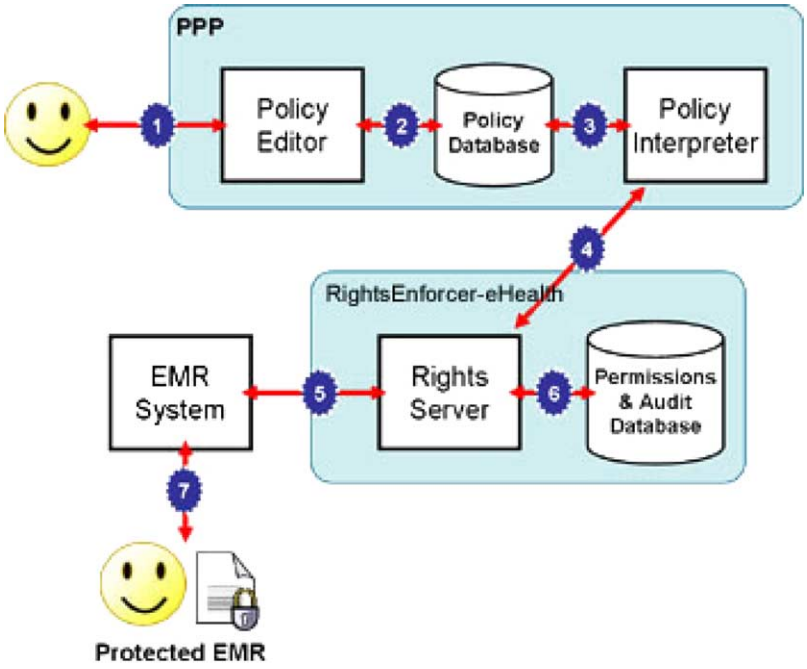

Fig. 1 Policy and Peer Permission process describing access and authorisation to an electronic medical record (EMR) through rights enforcer (RE) technology. A policy author uses PPP to write policy (Steps 1 and 2). Later a medical worker attempts to read a protected EMR (7), prompting the question to RE ''Does this user have the right to display this EMR?'' (5). RE may have a still-current answer saved from a recent query (6). (RE supports offline use.) If not, RE poses the same question to PPP (4), which interprets policy in an attempt to answer positively (3). The answer is saved in the Permissions database (6). All use is tracked in the same database (6).

giving it the ability to scale to thousands of users in a more manageable way [2]. The project has developed software (RightsEnforcer^{TM}) and a 'starter set' of workable policy statements for a deployable, rules-based, system to manage the access to, and use of, EHR's by health care professionals in the dynamic environment of healthcare (Fig. 1).

5. Canada Health Infoway Incorporated (CHII)

In 2001 the Government of Canada committed to an investment of $ 500 million to accelerate the development and adoption of modern systems of information technology. The culmination of this funding initiative was the founding of the Canada Health Infoway Incorporated (CHII or 'Infoway') in 2002 [3]. CHII is intended to be a facilitator and strategic investor, not a granting body. Its Board consists of the Federal, Provincial, and Territorial First Ministers of Health who, in September 2000, agreed to ''work together to strengthen a Canada-wide health infostructure to improve the quality, access, and timeliness of health care for Canadians.''

The mandate of CHII is to accelerate the pan-Canadian development and adoption of electronic health information systems with compatible standards and technologies. Within this mandate the immediate focus has been identified as seeking and implementing electronic health record (EHR) solutions. The concept of an EHR varies, and to ensure a consistent understanding, CHII has described an EHR as a record that is available electronically to authorized healthcare providers and to the individual patient anywhere and anytime, in support of high-quality care. It is intended to provide individuals in Canada with a secure and private lifetime record of their key health history and care within the health system.

In creating functionality and a 'value chain' for the EHR, four 'Generations' are envisioned for the projected evolution of the pan-Canadian EHR. Generation 1 constitutes the foundation, Generation 2 the documentor, Generation 3 the helper, and Generation 4 the mentor. Generation 1 activities include developing an architecture, registries, community survey, and physician and consumer research. Generation 2 focuses on laboratory and diagnostic imaging projects. Generation 3 is the pharmacy initiative. These Generations are not considered to be consecutive stages, since aspects of each can overlap or occur simultaneously. Such a structured approach is anticipated to reduce the

ultimate cost for the pan-Canadian EHR from $ 2.5—4.1 billion or more to just $ 1.3—2.2 billion.

Within the next 12—18 months it is intended to develop a detailed solution architecture, roll out a Canada-wide provider and client registry, and to establish pilot activities in terms of drugs (Generation 3 activity) and laboratory components (Generation 2 activity). In addition, diagnostic imaging pilots (Generation 2 activities) will be undertaken in community and acute care settings, a phase II national registry survey will be conducted, and attitudes of consumers to an EHR and privacy, and of physician attitudes to technology and EHR solutions, will be researched.

More recently, in the 2003 budget, the Canadian government provided CHII with an additional $ 600 million, and reaffirmed that their mandate included support of telehealth activities.

6. Glocal e-Health Policy Grid

Many policy issues have been identified including confidentiality and the patient's rights of access [13,14], data protection and security [15,16], malpractice [17], intellectual property [18], product liability and jurisdictional problems [19], risk management [20], and licensing [21,22]. A full understanding of the entire spectrum of e-Health Policy issues, their interrelatedness, and their glocal relevance is lacking.

An interdependence exists between all nations and there is mutual benefit to a networked flow of health information and knowledge amongst and between countries. There is therefore value in developing practical tools with which to guide both research and debate in the Glocal e-Health Policy arena. Policy experience within the Global e-Health Research and Training Program of the Health Telematics Unit has been growing [6,23,24]. Currently eight policy *levels*, nine policy *themes*, and eight policy *actor* categories are recognised, and an initial attempt has been made to describe these in terms of a two dimensional Glocal e-Health Policy Grid (Table 1). This grid is now being developed through empirical research to create a three dimensional Glocal e-Health Policy Matrix Model, intended to guide Glocal e-Health Policy development and identify key policy issues at each point of intersection within the matrix.

7. Global and 'glocal' perspective

e-Health is in place in most developed countries, and is being explored in many developing, even least developed, countries. Many practical issues will arise as global e-health becomes a reality, but of these the most critical may be policy [25]. Policy determines the rate and direction of development of healthcare initiatives, yet the vast majority of the world's countries have no legislation, e-Health Policy, or even guidelines [26]. For the foreseeable future e-Health Policy will remain the sole domain of individual countries, leading to 'domestic' solutions. This is of concern if a 'borderless' global e-health world is to be achieved. Inappropriate local, domestic, or international policy developed and implemented in any single jurisdiction may hamper or even cripple the ability of global e-health to fulfill its potential. Taking a glocal view in the development of individual initiatives will minimise this threat and its future impact.

The policy issues around e-health have been known for many years. A recent report identified at least eight countries that have national health information and technology strategies either in place or being developed: Canada, UK, New Zealand, USA, Italy, France, Japan, and Germany [27]. In other work, 20 countries were identified as having some defined e-Health Policy or clear policy activity [6].

Yet no single country has a pro-actively developed, comprehensive e-Health Policy environment. Malaysia is closest, and is unique in having a 20-year ICT plan termed the Multimedia Super Corridor (MSC) initiative, of which telehealth is a 'Flagship Application'. As a result, Malaysia is the only country to have proactive, moderately comprehensive, structured policy, with a Telemedicine Act—1997, Digital Signature Act—1997, and Communication and Multimedia Act—1998 amongst other 'Cyberbills' [28], and specific National Telehealth Policies—2000 covering; MACRO Telehealth Policies, Teleconsultation, Continuous Medical Education, Mass Customised Personalised Health, Information System Life Health Record, and Life Health Plan [29].

Given that the developing world represents about 80% of the global population, and given the rapid global growth of ICT and e-health, policy and other solutions being developed now in individual jurisdictions would greatly benefit from adoption of a glocal perspective.

8. Privacy policy as a case study

Proactive Glocal e-Health Policy development is desirable, however to this point policy that impacts global e-health has been developed in individual jurisdictions, and often coincidentally and reactively. An example is, the European Union's (EU)

Table 1 HTU 'Glocal' e-Health Policy Grid

Policy themes (and examples of issues)	Policy levels							
	Patient/ provider	Community	Program	Organisation/ facility	Region	Province/ territory/ state	National	Global
Professional Credentialing; professional conduct; registration; reimbursement; licensure; accountability (for clinical decisions); scope of practice								
Operational Funding; clinical standards; scope of practice								
Institutional Accreditation; access; authorisation; training; certification; protection of personal health information; data collection and management; data quality								
Ethical Confidentiality; consent								
Legal Privacy; security								
Cultural Traditional medicine; health beliefs								
Commercial Intellectual property; copyright								
Communication Cross-border acceptance; common 'language'								
Interoperability Technical; professional; organisational (standardized and interoperable systems)								

Policy actors (and examples): International bodies (e.g. World Health Organisation (WHO), International Telecommunications Union (ITU), International Standards Organisation (ISO), World Bank); non-government organisations (charitable groups, private sector foundations); private sector (multinational corporations); governments (national, regional (e.g. province, state), local); institutions (hospitals (regional vs. rural), clinics, academic institutions); agencies (accreditation agencies); professional groups/associations (physicians, nurses, dentists, allied healthcare professionals (multiple), IMIA, CST, COACH); public (individual 'consumers', interest groups).

'Directive' [30], Canada's response—Personal Information Protection and Electronic Documents Act (PIPEDA) [31], and more recently the final privacy rule of the Health Insurance Portability and Accountability Act (HIPAA) in the USA which became enforceable on 14 April 2003 [32]. Each addresses privacy, confidentiality, and security aspects of the collection and electronic exchange of personal data, and therefore has relevance to access and authorisation for any global EHR. Similar legislation exists in other countries also.

In 1980 the Organisation for Economic Co-operation and Development (OECD) developed, for its member states, a set of guidelines for the protection of personal information. These 'Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' represented an *international consensus* on how best to balance effective privacy protection with the free flow of personal data. They were accepted by Canada in 1984. Then, in 1995 the European Commission established its own 'Directive', which was enforced in 1998. This Directive required countries trading with or doing business in EU countries to have a regulatory system in place to protect personal information, and required businesses to adhere to ''fair information practices''. Although well intentioned, the EU's approach contributed to creation of a reactive, and potentially restrictive policy development, in other countries. For example, Canada introduced its own PIPEDA legislation in 2001, and in turn required Provinces to either immediately develop their own equivalent legislation within 2 years or be beholden to the Federal legislation. Canada's PIPEDA, which satisfies EU requirements, also has implications for Canada—US exchange of personal data. As a direct consequence of these activities, the US hastily developed 'Safe Harbor' guidelines to deflect their impact.

This case study highlights the need for inter-jurisdictional efforts at Glocal e-Health Policy development.

9. Discussion

The ultimate goal is to have global access to EHR data by authorised personnel only. This requires access and authorisation policy and procedure that is stringent and effective, yet flexible and viable—and that is globally acceptable. The same is so for the other policy issues identified in the Glocal e-Health Policy Grid. But at this time, healthcare providers and organisations are in a quandary. e-Health is a reality and is being practiced locally and regionally, somewhat nationally, and even globally. Yet in Canada limited national or even Provincial or Territorial policy or regulations exist to guide the growing spectrum of e-health activity. The same is so for other countries, particularly in terms of inter-jurisdictional e-health. This void in leadership is a major concern, and is being plugged by development of policy and guidelines at the lower echelons.

Attempts to correct this situation are taking place in Canada. NIFTE will provide a firm base from which to structure national e-Health Policy development, and PPP will provide a practical software program to control access rights based upon workable policy statements and a unique persistent security approach to data. Together, these provide important first steps, and provide perspective upon which to build, particularly as CHII's initiatives unfold.

For example, a particular strength of the NIFTE guidelines is expected to be their emphasis on review of existing policy and procedure, and amendment of these to accommodate e-health. Given the desire to integrate e-health intimately into routine healthcare practice, this principle is most important. Only where essential should new and specific e-Health Policy and procedure be developed.

The NIFTE Guidelines will also provide evidence for areas of concern. For example, Draft 2 of the guidelines explicitly indicate that a necessary 'interim strategy' is to ''have interim policies, guidelines and agreements in place to deal with cross-jurisdictional telehealth services'' until such time as a national policy is developed. This is very practical advice under prevailing circumstances. But, when considered glocally this has the potential to create diversity of approach, and discontinuity in process. This realisation should stimulate coordinated national and Glocal e-Health Policy efforts.

Similarly, the draft NIFTE guidelines provide a 'suggested guideline' that ''a written agreement or contract between the healthcare organisations/institutions involved in telehealth services is in place and includes written statements appropriate to all relevant policy issues''. Again, this offers sage and practical advice. However, consider the networked and inter-jurisdictional nature of e-health—the potential exists for a single site to require multiple agreements with various combinations and permutations of content. Consider also the tendency for prolonged, costly negotiations in new and poorly defined areas with potential risk management and legal ramifications, i.e. e-health. There is potential for frustration and significant delay in providing appropriate and valuable e-health mediated healthcare, and for inadvertent creation of barriers to global e-health. This too should

stimulate coordinated national and glocal e-Health Policy efforts.

When preparing its 'Directive', the EU commented that ''If each member State had its own set of rules on data protection, for example on how data subjects could verify the information held on them, cross-border provision of services, notably over the information superhighways, would be virtually impossible.'' This astute comment speaks to the need for collaborative and proactive Glocal e-Health Policy development.

Glocal e-health framework and policy building cannot be addressed in the short term, but development of appropriate tools and a strategy to address this need is essential in the short to medium term. National efforts such as NIFTE and PPP support larger initiatives such as CHII, and provide some tools that can be emulated or adopted elsewhere, and the Glocal e-Health Policy Grid provides one component for a policy strategy. Together they provide a practical and research based approach that will identify and address relevant policy issues at various policy levels and for various policy actors.

10. Conclusion

Global e-Health is the natural culmination of our cumulative e-health efforts, and will bring tremendous change to our world through increasing access, and equity of access, to healthcare for most of the world population. To achieve this, there will be the need to utilise globally distributed healthcare records, and to have seamless inter-jurisdictional agreement on matters such as access and authorisation. This in turn requires that issues pertaining to policy and procedure be addressed 'glocally' and in a manner that effectively accomplishes knowledge transfer from the research to the policy sectors.

References

[1] NIFTE website, National Initiative for Telehealth Guidelines—http://www.nifte.ca, accessed 14 April 2003.

[2] PPP website, Policy and Peer Permission—http://www.rightsmarket.com/ppp/, accessed 14 April 2003.

[3] CHII website, Canada Health Infoway Incorporated. http://www.canadahealthinfoway.ca/.

[4] ISO/TC 215/WG 4. ISO/TC 215/WG 4—Security of Health Informatics Glossary (Rev 1)—Security and related definitions, International Standards Organisation (ISO), Geneva, Switzerland, 2000.

[5] ISO/IEC 2382-08, Security, second ed., International Standards Organisation (ISO), Geneva, Switzerland, 1998.

[6] R.E. Scott, M.F.U. Chowdhury, S. Varghese, Telehealth policy: looking for global complementarity, J. Telemed. Telecare 8 (2002) 55—57.

[7] M. Guillen, Is globalization civilizing, destructive, or feeble? A critique of five key debates in the social-science literature, Annu. Rev. Sociol. 27 (2001) 235—260.

[8] Impact of technology on global health: perspectives and promise. The Pfizer J. 5(2) (2001) 1—36.

[9] G. Berlinguer, Globalization and global health, Int. J. Health Services 29 (3) (1999) 579—595.

[10] Today's technological transformations—creating the network age, in: United Nations Development Programme; Human Development Report 2001—Making New Technologies Work for Human Development, Oxford University Press, New York, 2001, pp. 27—64.

[11] R.E. Scott, M. Palacios, e-Health—challenges of going global, in: C.M. Scott, W.E. Thurston (Eds.), Collaboration in Context. Institute for Gender Research and Health Promotion Research Group, University of Calgary, Calgary, Alberta, Canada, 2003, pp. 45—55.

[12] I. Kickbusch, Global + local = glocal public health [editorial], J. Epidemiol. Community Health 53 (8) (1999) 451—452.

[13] B. Stanberry, The legal and ethical aspects of telemedicine. 1. Confidentiality and the patient's rights of access, J. Telemed. Telecare 3 (4) (1997) 179—187.

[14] C. Pyper, J. Amery, M. Watson, C. Crook, B. Thomas, Patients access to their online electronic health records, J. Telemed. Telecare 8 (Suppl 2) (2002) 103—105.

[15] B. Stanberry, The legal and ethical aspects of telemedicine. 2. Data protection, security and European law, J. Telemed. Telecare 4 (1) (1998) 18—24.

[16] S.A. Buckovich, H.E. Rippen, M.J. Rozen, Driving toward guiding principles: a goal for privacy, confidentiality, and security of health information, J. Am. Med. Informatics Assoc. 6 (2) (1999) 122—133.

[17] B. Stanberry, The legal and ethical aspects of telemedicine. 3. Telemedicine and malpractice, J. Telemed. Telecare 4 (2) (1998) 72—79.

[18] D. Beauregard, G. Beauregard, The intellectual property cookbook: a guide for the novice health-care telemedicine provider working with industry, J. Telemed. Telecare 6 (1, Suppl 1) (2000) 107—109.

[19] B. Stanberry, The legal and ethical aspects of telemedicine. 4. Product liability and jurisdictional problems, J. Telemed. Telecare 4 (3) (1998) 132—139.

[20] S. Wallace, L. Sibson, B. Stanberry, D. Waters, P. Goodall, R. Jones, J. Evans, R. Dunn, The legal and risk management conundrum of telemedicine, J. Telemed. Telecare 5 (Suppl 1) (1999) 8—9.

[21] L.E. Nohr, Global medicine and licensing, J. Telemed. Telecare 6 (1, Suppl 1) (2000) 170—172.

[22] P.D. Jacobson, E. Selvin, Licensing telemedicine: the need for a national system, Telemed. J. e-Health 6 (4) (2000) 429—440.

[23] P.A. Jennett, D.P. Kulas, D.C.M. Mok, M. Watanabe, Telehealth: a timely technology to faciltate health decision making and clinical service support, in: J.K.H. Tan, S. Sheps (Eds.), Health Decision Support Systems. Aspen Publishers, 1998, pp. 353—369.

[24] P. Jennett, B. Seidlecki, Telehealth policy: building a functional system, Telehealth Law 1 (4) (2001) 53—58.

[25] M. Rigby, K. Birch, R. Roberts, The need to ensure that the globalization of information and telematics does not destabilize health-care worldwide, J. Telemed. Telecare 6 (1, Suppl 1) (2000) 116—118.

[26] M. Loane, R. Wootton, A review of guidelines and standards for telemedicine, J. Telemed. Telecare 8 (2) (2002) 63—71.

[27] F/P/T Advisory Committee on Health Infostructure, Blueprint and Tactical Plan for a pan-Canadian Health Infostructure—A Report on F/P/T Collaboration for the Planning of the Canadian Health Infostructure. Office of Health and the Information Highway, Health Canada, Ottawa, December 2000.
[28] MyCERT, http://www.mycert.mimos.my/ > Malaysian Cyberbills, accessed 14 April 2003.
[29] Ministry of Health Malaysia, http://www.telehealth.com.my/ > Policy, accessed 14 April 2003.
[30] The Directive, 1995, The European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, July 1995.
[31] HIPAA, The Health Insurance Portability and Accountability Act of 1996, Office of the Federal Register (OFR), USA.
[32] Office for Civil Rights, Health and Human Services. Standards for privacy of individually identifiable health information. Final rule, Fed. Reg. 67(157) (2002) 53181—53273.