INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 76 (2007) 402–406

journal homepage: www.intl.elsevierhealth.com/journals/ijmi

# Secure e-Health: Managing risks to patient health data

*Eike-Henner W. Kluge**

*Department of Philosophy, University of Victoria, Victoria, BC, Canada V8W 3P4*

ARTICLE INFO

*Keywords:*
e-Health
Security
Privacy
Harmonization
Information ethics
*USA Patriot Act*
Electronic health record
Codes of ethics

ABSTRACT

e-Health, as an inter-jurisdictional enterprise, presents risks to patient health data that involve not only technology and professional protocols but also laws, regulations and professional security cultures. The *USA Patriot Act* is one example of how national laws can shape these concerns. Secure e-Health therefore requires not only national standardization of professional education and protocols but also global interoperability of regulations and laws. Some progress in this regard has been made in the European context; however, even here developments are incomplete, and nothing similar has been accomplished on a global scale. Professional health information organizations must take the lead in developing appropriate high-level principles for professional certification and security protocols and in harmonizing these on a global basis, so that they can provide a firm and consistent foundation for international treaties. Such developments should occur in concert with other health professions, so that coordinated requirements are integrated into revisions of the relevant codes of ethics. This presentation identifies and addresses some of the ethical and legal issues and proposes a series of recommendations.



## 1. Introduction

e-Health, with its promise of efficiency and cost-effectiveness, has become a valued tool in private and public health care. However, it was recognized from the very beginning that it presents a variety of problems that range from privacy and security issues to reliability, quality control, accessibility and usability [1]. Portability and integration are also implicated [2]. Over the last few years, most of these problems have received considerable attention and various methods for dealing with them have been explored. Attention has also focussed on informed consent to data collection [3–10], exchange protocols [11–13], and the standardization of electronic health record (EHR) structures and architectures. Another focus has been the interoperability of networks [14], the standardization of nomenclatures, syntax and semantics [15–18], and the development of codes of ethics for health information professionals (HIPs) and e-Health practitioners [19–22]. In fact, a concern for ethics seems to have been integral to the evolution of e-Health from the very beginning.

However, there are several issues, which unless appropriately addressed, may well undermine continued ethical development. *First*, there is the apparent subordination of international ethical standards to individual state interests. The *USA Patriot Act* [23] here constitutes the most flagrant example. *Second*, there is a glaring absence of international agreement on ethically appropriate mechanisms to ensure the qualification of the HIPs who actually deploy and manage this technology and on the enforceability of appropriate standards. *Third*, there are currently no moves to develop similar standards governing the qualification and training of health care professionals (HCPs) and administrators in this domain. *Fourth*, and perhaps most importantly, there is no global agreement on the precise status of health records and on the basic *raison d'être* of health care itself. I shall consider these in turn and discuss their relevance and implications. I shall con-

* Tel.: +1 250 721 7519; fax: +1 250 721 7511.
E-mail address: ekluge@uvic.ca.
1386-5056/$ – see front matter © 2006 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.ijmedinf.2006.09.003

clude with some tentative suggestions for ameliorating the situation.

## 2. National interests and ethical standards

### 2.1. *The USA Patriot Act and its implications*

The threat presented by the subordination of international ethical standards to individual state interests is most glaringly illustrated by the *USA Patriot Act*. This *Act* allows the Federal Bureau of Investigation and the National Security Agency of the United States to make application to the United States Foreign Intelligence Surveillance Agency Court (FISA Court) for an order to compel the production of any business record or tangible things from anyone under the jurisdiction of the United States, including foreign subsidiaries of US corporations, for any investigation that is alleged to protect the United States against international terrorism or clandestine intelligence activities. The standard of proof required in such applications is not that of reasonable doubt but of perception in the eyes of the applying agency, and §215 of the same *Act* prevents anyone from notifying the subjects of the records that an invasion of their privacy is being contemplated or has occurred [23,24]. The FISA Court generally grants such requests [24,25]. The *Act*, therefore, essentially gives US government agencies the right to abrogate the privacy rights, including EHR privacy rights that are otherwise firmly entrenched.

At first glance, this may seem irrelevant for the development and deployment of e-Health on a global scale since the legislation only applies to US corporations and agencies. However, in an era where health care as well as informatic services are provided by multinational corporations that have US parent corporations and affiliates, the threat to privacy expands to the global arena. It essentially means that anyone who has formal US connections or provides professional health services cannot protect the privacy rights of their patients, their own national laws notwithstanding, and that a telecommunication provider or corporation that utilizes or manages EHRs and is associated with a US agency can no longer guarantee the privacy of the records it handles. Arguably, therefore, if the potentials inherent in e-Health are to be fully developed, either the *Act* has to be repealed or some way has to be found to ensure privacy despite this legislation.

Some jurisdictions that have contracted with subsidiaries of US corporations – for example, British Columbia, which has contracted with Maximus BC (a subsidiary of a US-based corporation) to provide records services to the Ministry of Health – have attempted to deal with this threat by legislating that health records in the possession or under control of a US corporation or affiliate may not be exported or in any way communicated to a US agency without explicit permission from the BC Ministry of Health. However, such legislation is ineffective because the *USA Patriot Act* prevents corporations from informing anyone if records in their possession or under their control have been subpoenaed and accessed by US security agencies.

Another solution that has been suggested is encryption. Encryption is of course desirable in its own right, and in fact is standard practice in record communication [14]. However, to avoid the impact of the *Patriot Act*, this would require that encryption keys not to be communicated, which would rule out precisely what makes e-Health so attractive in the first place, namely consultation with centres of excellence located in or affiliated with the US. After all, the relevant communications would have to be decrypted in order for the consultation to proceed. With due alteration of detail, similar considerations apply to US-affiliated health care providers and insurance agencies.

### 2.2. *Issues of ethical principle*

The preceding highlights a specific threat that is posed by legislation such as the *USA Patriot Act*. On a more general level, the issue goes much deeper. This kind of legislation subordinates ethical standards and traditions to the pragmatics of national interests. Its significance, therefore, extends beyond the particulars of any such *Act*. It raises two fundamental questions: *First*, should problems that arise in different areas of social concern be allowed to overrule the standards that are otherwise appropriate for the delivery of health care? *Second*, should problems that arise in the design and delivery of health care, and in particular in the design, construction and use of health information systems, be solved by focusing on what is practical and promotes the greatest good for the greatest number, or should solutions be sought within the limits of fundamental ethical principles?

A satisfactory answer to the first question requires a decision about the relationship between health care and other social undertakings. Is health care special? If so, does it mean that the ethical standards that are appropriate in health care, inclusive of privacy and security (which have been integral to health care from its very beginnings), are immune from outside pressures? These are fundamental questions that transcend the scope of the present discussion. However, they have to be resolved if regulatory structures that surround e-Health are to be more than merely ad hoc devices.

The second question, although closely related to the first, has a more pragmatic focus. It acknowledges that no rights are absolute, but that all have limitations. In that sense, an answer to the second question provides at least a partial answer to the first. Both logic and ethics agree that if ethical rights have limits, then these limits must be drawn consistently with the very logic of ethics itself. In other words, it means that any abrogation of specific rights – inclusive of informatic rights – must be consistent with the fundamental principles that define the domain of ethics. It therefore means that the ends do not justify the means, and that ends must be achieved only through measures that are consistent with the ethical principles that justify the ends in the first place.

This immediately highlights the fact that any appeal to the greatest good for the greatest number is incomplete without an identification of the nature of that good. Arguably, to define the greatest good for the greatest number independently of ethical considerations is to adopt a materialistic perspective that is antithetical to the very ideas that underlie the insistence that privacy is a fundamental human