THE HEALTH INFORMATION PROFESSIONAL IN EHEALTH:ETHICAL CONSIDERATIONS FOR AN INTERJURISTICAL SETTING

Eike-Henner W. Kluge
University of Victoria, Victoria, BC, Canada
E-mail:ekluge@uvic.ca

Abstract: Issues such as privacy, security, quality, etc. have received considerable attention in discussions of eHealth; however little attention has been paid to the fact that eHealth situates health information professionals (HIPs) in an ethical and legal context that differs importantly from that of traditional health care. In traditional health care HIP services are pragmatically useful but not inherently necessary; in eHealth, however, HIPs are not only the interface between physicians and patients but the instrumental facilitators of eHealth itself. With this, their professional standing acquires a fiduciary parameter it did not have before, and older models of the ethics of health information professionals are no longer wholly sufficient to provide guidance. Matters are complicated further by the inter-jurisdictional parameters of eHealth, which introduce dimensions that do not exist in the traditional intra-jurisdictional setting. This paper outlines the issues and sketches a possible approach for addressing the situation.
Keywords: eHealth, ethics, health information professionals

Introduction

eHealth is a quintessential paradigm of technology transfer and, according to common perception, it does not raise new ethical or legal issues for health information professionals (HIPs). Privacy, security and confidentiality—which are of special concern for HIPs in eHealth—had already been identified as ethically and legally important issues when electronic diagnostic and imaging technologies first came on the scene, and the role of HIPs in this regard had been carefully considered. Likewise, the ethical and legal issues surrounding electronic health records (EHRs) and of the communication technologies that are integral to eHealth were also subjected to intensive ethical and legal scrutiny when they were first introduced, and the ethical position of HIPs had been carefully outlined in relevant regulations and codes of ethics. Any new issues that have arisen with eHealth—so the argument— are merely the result of the increased complexity of the electronic devices, tools and methods of communication that have come into play, and therefore involve only technical matters. The ethical and legal fundamentals that have guided HIPs in the past have remained essentially the same; therefore there is no need to subject the ethical position and role of HIPs to special scrutiny.

The Changing Ethical Framework of eHealth

This understanding, however, fails to appreciate the fundamental changes in the overall ethics of health care that have been brought about by eHealth and the implications these changes have for both physicians and health care professionals. For instance, the fiduciary physician-patient relationship, which is definitive of medicine, became divorced from the direct physician-patient interaction that grounded it in the traditional setting and became grounded in a virtual rather than a real interaction; the EHR, which hitherto had been a pragmatic device that could in principle be dispensed with, (Gunter and Terry, 2005; Patel, Jamoom, Hsiao, Furukawa and Buntin, 2013; Xieali et al., 2013) became an indispensable tool without which physicians could not function; and HIPs, rather than being mere service providers, became integral causal player without whom the physician-patient relationship could not arise and eHealth itself could not come into existence. The ethical implications of these changes became especially noteworthy when eHealth began to cross jurisdictional boundaries.

What all of this this means for physicians has already been explored elsewhere. (Kluge, 2014) The focus of this discussion is the implications for HIPs. Among other things, it will be argued that HIPs acquired a fiduciary relationship towards patients they did not have before, that this relationship has human rights implications, and that the relationship between HIPs and their corporate employers has to be reassessed in order to provide a complete picture.

EHRs, Communication Technology and eHealth

To fully appreciate what is at stake, it may be appropriate to begin with the fundamental role of EHRs in eHealth and the implications this has for the ethical status of HIPs.

EHRs themselves may be viewed either materially or informatically. Viewed materially, they are sets of electronic patterns that capture multimedia data and that can be transmitted, received, stored, retrieved, linked or otherwise manipulated for various purposes, the primary one being to provide health care. From this perspective, the issues that are associated with EHRs are purely technical in nature. They include such things as technical standards and product suitability, quality, reliability, security, usability, etc. (International Standards Organization, 18308 and 20514) Any legal or ethical concerns that might arise when viewed from this perspective are inherently technical in nature and essentially centre in contractual considerations. (United Nations, 1980)

By contrast, when viewed informatically, EHRs are sets of health data that can be linked to specific patients because of the relationship in which they stand to the patients. Another way of putting this is to say that, informatically speaking, EHRs are patient-relative data-spaces that function as the informatic and epistemic foundations of the patient profiles that are developed by health care professionals (HCPs) and that are used to develop diagnoses and make treatment decisions. (Kluge, 2001)

The Existential Role of EHRs in eHealth

In contrast to traditional health care, in eHealth EHRs and communication technology are not simply tools that physicians may or may not use, where failure to use them only has quality-of-service implications. In eHealth, neither diagnostic nor therapeutic work is possible without them and physicians cannot function as physicians. However, it is HIPs whose work underwrites the possibility of EHRs and of the technology that maintains and transmits them—and with this, HIPs have become integrally involved in the physician-patient interaction itself: not as a matter of choice or quality improvement but as a matter of existential necessity. Therefore while in traditional health care the basic relationship was a dyad consisting of physician and patient, in eHealth it has become a triad consisting of physician, patient and HIP. The fact that HIPs do not provide therapeutic services in eHealth is ethically irrelevant. What is important is that HIPs are the causal agents who make the physician-patient interaction itself possible in the first place.

The point is worth repeating. The use of EHRs is not a matter of pragmatic convenience or of professional excellence in eHealth, as it is in traditional health care. Traditional health care proceeds perfectly fine without EHRs, and the physician-patient relationship does not depend on them for its inception. With eHealth, however, EHRs have become a matter of causal necessity. Without them, there cannot be any diagnostic or therapeutic physician-patient interaction, and the physician-patient relationship cannot even come into existence. Moreover, not only EHRs but also the communication framework that makes diagnosis and treatment possible —in a word, the whole framework of eHealth itself—depends on HIPs. With this, HIPs ceased to be merely technical agents and their ethical status acquired a fiduciary element towards patients that in important ways is analogous to that of physicians.

Privacy Rights, Human Rights and eHealth

The use of EHRs in eHealth immediately entrains privacy considerations, and when combined with the causal role of HIPs that was just pointed out, this immediately changes the strength of HIPs' privacy obligations.

Privacy and, correlatively, confidentiality concerns are of course as old as Hippocrates, (Higgins, 1989) and have been addressed in medical codes of ethics as long as such codes have existed. The codes have always emphasized privacy and confidentiality, and have always taken special care to extend this to patient records when patient records were first formally kept for therapeutic purposes. (Kahn, 1970; Siegler, 2010)

Although traditional, privacy rights were first explicitly enunciated on an international and interjurisdictional scale in 1948 in Article 12 of the Universal Declaration of Human Rights. (United Nations, 1948) The Declaration stipulates that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Privacy rights, therefore, being fundamentally grounded in the domain of human rights, are independent of national juridical provisions, international trade agreements or institutional guidelines.

It is this that changes the picture for HIPs in eHealth. Reason suggests that persons who are instrumentally involved in the violation of a right cannot escape responsibility merely because they are not directly and personally engaged in the act itself. The instrumental, facilitating and enabling involvement as distinct from merely providing the tools is sufficient to trigger complicity. This is not simply a matter of logic or ethics but also finds reflection in legal pronouncements and decisions. (Federal Republic of Germany, 19:3; International Criminal Tribunal, 2004-2006; People's Republic of China, II:36) HIPs are instrumentally involved in the conduct of eHealth in this very sense. It therefore follows that any violation of patient privacy rights that occur in eHealth—say, in intelligence gathering when EHRs are accessed for security or other non-medical purposes—will implicate HIPs. They are co-determinative of the causal flow of events that constitutes eHealth, and hence they share in responsibility.

All of this assumes cardinal importance when eHealth crosses international borders—for instance, when the eHealth providers who employ the HIPs store the EHRs that are used in their system in jurisdictions other than those where the service is actually delivered (cloud storage) (Chen et al., 2012), or when the providers are incorporated in jurisdictions like the USA where provisions like the USA PATRIOT Act (USA Patriot Act, 2001) apply to the parent corporations and by extension are assumed to apply to their subsidiaries. In the first sort of case, the privacy rights of patients in the jurisdiction-of-delivery may be different from those of the jurisdiction-of-storage, and what is legal with respect to use—for instance for research purposes—may differ in the respective jurisdictions. HIPs who are instrumentally involved in eHealth that fits this pattern and who do not ensure that the patients of the relevant eHealth system are informed of this possibility will be ethically complicit in any violation of the patient privacy rights in the jurisdiction-of-delivery even though they themselves are not involved relative to the content of these actions. The notion of complicity still applies.

In the second sort of case, the legal provisions in the provider's jurisdiction-of-incorporation may stipulate that EHRs may be accessed by security forces without patient consent or knowledge. Therefore while the actions of the HIPs as facilitators (and of the corporations as employers and service providers) may be considered ethical and legal in the parent corporation's jurisdiction-of-incorporation, they may not be considered ethical or legal in the jurisdiction-of-delivery. Some of the concerns that have been raised about US corporate eHealth providers relative to the ethical and legal considerations that apply in European countries point in that direction, the so-called Safe Harbour agreements notwithstanding, (Commission of the European Union, 2014) and they raise ethical (and legal) concerns for HIPs engaged in inter-jurisdictional eHealth.

Further Considerations

What has just been outlined does not, of course, present the full extent of the HIP's ethical role in eHealth. There is also the fabric of duties they have towards the employers who underwrite eHealth as a business. They include fit-for-the-purpose considerations and extend to ensuring that the systems in which eHealth is delivered function consistently, reliably and in the best possible way without imperilling the commercial success of the eHealth enterprise. While these and related duties existed before the advent of eHealth, they acquired increased importance because of the integrally causal role of HIPs in eHealth itself; and while they are addressed in current codes of ethics for HIPs, (International Medical Informatics Association, 2002) these latter were originally formulated for the traditional health care context and do not provide entirely satisfactory guidance in the eHealth setting.

Codes of Ethics and Other Considerations

All of this raises the question what reflection any of this should find in ethical and legal provisions—especially when eHealth transcends juridical boundaries. The issue itself has two sides. On one side is the question of how to structure relevant provisions in a formal ethical code that acknowledges the novel position of HIPs in eHealth; on the other side is the question of how to operationalize this in terms of pragmatically workable features that make a difference in actual practice.

As to the first, the foundational provisions of the IMIA Code of Ethics for Health Information Professionals of course continue to apply even in the eHealth context because the underlying ethical principles that govern the actions of HIPs have not changed. What has changed is the HIPs' role and function. Whereas previously HIPs occupied a subordinate role as provider of technical services, with eHealth they became the causal foundation of health care and became pivotal to its inception and delivery. Therefore what is required are not new principles but a new framework for implementing the principles—particularly since, as has been emphasized, eHealth in its expanded version is inter-jurisdictional in nature.

An integral step in achieving this—which in turn is based on the acknowledgment that HIPs operate in a corporate setting—would involve ensuring that the corporate eHealth framework in which HIPs work is itself ethically structured. This would ensure that HIPs can function in an ethically appropriate manner. However, since the focus of this discussion is not the corporate framework of eHealth but the ethical issues that face HIPs in the eHealth setting, it is not necessary to expand on this aspect of the issue. Moreover, the matter is specifically dealt with elsewhere. (Croll, Ruotsalainen, Kluge, Lacroix & Sahama, 2015)

As to HIPs, the aim could be achieved by establishing a globally accepted certification and accreditation structure for HIPs who wish to work in eHealth in an interjurisdictional setting. Such a structure would be headed by an international body under the auspices of the WHO. The membership of this body would be drawn from such organizations as the national health informatics associations who are members of IMIA, as well as from the Council of European Professional Informatics Societies, the Asia-Pacific Association of Medical Informatics, the International Conference of Data Protection and Privacy Commissioners and related international organizations.

The function of this body would be threefold: to set international standards of technical proficiency and ethical understanding for HIPs, to certify health information professionals as meeting these standards, and to monitor and adjudicate profession-related issues from an inter-jurisdictional perspective. The technical certification process could be based on the model that was developed by Belgium for certification of health informatics professionals, which in turn could be adapted with reference to the protocols that are used by the European Computer Driving Licence Foundation in its technical certification programme.(European Computer Driving Licence Foundation, 2015) It would have both a technical and an administrative competence focus, and would be regularly updated as the technology evolves and administrative parameters change in the international setting. Ethical understanding and competence would an integral part of the required skill-set necessary for certification. Sufficiency and competence in this regard would be measured with reference to ethical guidelines that would be based on the IMIA Code of Ethics for Health Informatics Professionals and addenda specific to HIPs engaged in eHealth. In order to ensure continued competence as the international context of eHealth evolves and develops, certification would be on a limited-time basis and would require evidence of maintenance of competence similar to the model that exists for physicians and other health care professionals in many jurisdictions relative to their medical specialty. Certification would be a fee item, which latter would fund the operation of the certification structure itself.

Finally, any matters of conflict that might arise with respect to these and related issues would be resolved by an adjudication process that was conducted by an independent body, also under WHO auspices and along the lines of the United Nations Commission on International Trade Law (United Nations, 1966), where membership was drawn on a rotating basis from members of IMIA. Identification of the relevant individuals from member organizations would fall to the member organizations themselves. This body would be funded by countries subscribing to the certification process itself.

Conclusion

eHealth situates HIPs in a novel ethical and legal context which in some respects importantly differs from that of traditional health care. This does not mean that the traditional ethical and legal provisions for HIPs have lost their relevance. Traditional methods of health care delivery continue to exist side-by-side with eHealth, and HIPs continue to operate in this established setting. However, the new roles that HIPs play in eHealth setting cannot be accommodated by adding technical fixes to current ethical and legal provisions. That would be to assume that technical fixes are answers to ethical (and legal) problems. What is required is an expanded set of guidelines and regulations. The preceding discussion has outlined why and how this is the case. It has also emphasized that because of the interjurisdictional aspects to eHealth, merely national adjustments will amount to no more than patchwork solutions to a problematic that has global dimensions. It remains to be seen whether this situation will be dealt with in a piecemeal or an all-embracing and consistent fashion.

References

Chen, T.S., Liu, C.H., Chen, T.L., Chen, C.S., Bau J.G., Lin, T.C.. (2012). Secure dynamic access control scheme of PHR in cloud computing. *Journal of Medical Systems, 36,* 4005-20. doi: 10.1007/s10916-012-9873-8.

Commission of European Communities. (2014). *The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles.* Retrieved 15/05/2015 at http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf.

Croll, P.R., Ruotsalainen, P., Kluge, E-H., Lacroix, P. & Sahama, T.,(2015). The global protection of personal health data. *Proceedings of the 15th World Congress on Health and Bioinformatics* (MedInfo 2105: Brazil, forthcoming).

European Computer Driving Licence Foundation. (2015). *ICDL*. Retrieved 19/05/2015 at http://www.ecdl.com/.

Federal Republic of Germany. *Grundgesetz*, Art. 19, Abs. 3.

Italy. *Costituzione della Republica Italiana*, Art. 39, Par. 4.

Gunter, T.D. & Terry N.P. (2005). The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions. *Journal of Medical Internet Research, 7*: e3.

Higgins, G.L. (1989). The history of confidentiality in medicine. *Canadian Family Physician*. *35*, 921-926.

International Medical Informatics Association. (2002). *The IMIA Code of Ethics for eHealth Information Professionals*. Retrieved 15/05/2015 at http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf.

International Criminal Tribunals. (2004). *Judgment in Kordic* (IT-95-14/2) Appeals Chamber.

International Criminal Tribunals. (2006). *Judgment in Mpambara* (ICTR-01-65-T) Trial Chamber.

International Standards Organization. ISO/TS 18308 and ISO 20514.

Kahn, A.P. (1970). From Ben Franklin's vision to medical record reflections. *Medical Records News,* 42-55.

Kluge, E-H. (2001). *The ethics of electronic patient records.* New York and Bern: Peter Lang.

Kluge, E-H. (2014).The Physician-Patient Relationship in eHealth. *Proceedings of the 8th Multi-Conference on Computer Science and Information Systems*, 399-402. Lisbon: International Association for the Development f the Information Society.

Patel, V., Jamoom, E., Hsiao, C.J., Furukawa, M.F. & Buntin, M. (2013). Variation in electronic health record adoption and readiness for meaningful use: 2008-2011. *Journal of General Internal Medicine, 28*, 957-64.

People's Republic of China. *General Principles of Civil Law*, Ch. III Art 36 f.

Siegler, E.L. (2010(. The evolving medical record. *Annals of Internal Medicine, 153*, 671-7.

United Nations. (1966). Resolution 2205 (XXI) of 17 December 1966.

United Nations. (1980). *Convention on Contracts for the International Sale of Goods*. Vienna: United Nations.

United Nations. (1948). *Universal Declaration of Human Rights*. NY, New York: United Nations.

USA. (2001). PATRIOT Act: PUBLIC LAW 107–56. Retrieved 15/05/2015 at http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html.

Xierali IM, Hsiao CJ, Puffer JC, Green LA, Rinaldo JC, Bazemore AW, Burke MT, Phillips RL Jr. (2013). The rise of electronic health record adoption among family physicians. *Annals of Family Medicine, 11*, 14-9.

