

## **The IMIA Code of Ethics: Revision 2016** ***Health Information Professionals and eHealth***

*Eike-Henner W. Kluge, SiHIS and University of Victoria*

### **Introduction**

Codes of professional ethics are fundamentally different from statements of legally mandated rights and obligations. Legal provisions provide the regulatory framework within which a profession carries out its activities but they do not always address ethical issues. Moreover, legal provisions are formulated by legislators, judges, or juries with reference to current and anticipated circumstances as these are understood at a particular point in time. Therefore they are time-bound and can provide little guidance when unexpected technical developments occur or when new types of situations arise. Moreover, they are jurisdiction-specific and hence, unless enshrined in trade agreements or international treaties, are of uncertain applicability in the global setting.

By contrast, codes of professional ethics are grounded in fundamental and generally accepted principles of ethics which latter, as the *Universal Declaration on Human Rights*<sup>1</sup> amply illustrates, are jurisdiction-invariant. Codes of professional ethics, therefore, when properly constructed, are the application of these principles to the domains of the relevant professions. Therefore they are independent of the vagaries of the judicial process, treaties, or formal agreements and, rather than following these, may well guide them; and rather than becoming invalidated by changes in technology or administrative fashion, may well indicate the direction in which these developments should proceed.<sup>2</sup> They can therefore provide guidance in times of legal or administrative uncertainty and in areas where relevant laws or administrative provisions do not yet exist. In so doing, they can assist in defining the ethical landscape.

At the same time, it would be inappropriate for a code of ethics—and the IMIA Code of Ethics for Health Information Professionals (HIPs) is no exception—to try to address every possible situation that might arise. In the first place, it presupposes that it was possible to identify them all, which is not the case. Moreover, it would make the resultant code too unwieldy for actual practice. Instead, a properly constructed code of professional ethics will focus on the types of ethical situations that typically arise in the conduct of the profession. In so doing, it will leave room for professional judgement and thereby acknowledge that otherwise identical situations may differ in their ethical implications because of the differences in their social embedding. Furthermore, a properly constructed code will generally be unaffected by changes in the technical

---

<sup>1</sup>[http://www.ohchr.org/EN/UDHR/Documents/UDHR\\_Translations/eng.pdf](http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf).

<sup>2</sup>Compare the influence of ethical consideration on the formulation of the European Data Protection Directive (Directive 95/46/EC) and on the revision in the forthcoming General Data Protection Regulation which is also guided by ethical considerations.

tools, devices, or methodologies that are used by the professionals because these usually do not affect the ethics of the professional-client relationship itself.

But that is not always the case. Sometimes the introduction of a new technical tool or device, an alteration in the way professional services are provided, or a shift in the social embedding of a profession can transform the ethical framework of the profession itself. Unless such a change is identified, acknowledged, and assimilated, the code will have only limited applicability and provide only limited ethical guidance in the new context. It is therefore important that codes of professional ethics be reviewed on a continual basis. Only that will ensure that emerging matters of ethical significance are adequately addressed in a timely manner.

These considerations are especially important in the case of health informatics. Health informatics is the discipline that deals with how health data are collected, stored, manipulated, communicated, and processed into health information that is suitable for administrative and clinical decision making, and with how computer and telecommunications technology are applied to support the delivery of health care services. HIPs are therefore important players in contemporary health care. Contemporary health care, however, is constantly evolving not merely in the clinical sense but also with respect to the informatics tools it uses and on which it relies. This means that the HIP's domain of activities is also in a state of continual flux—which in turn means that the code of ethics that guides the conduct of HIPs should regularly be examined to ensure that the guidance it provides is current and that the advice it offers is useful and in keeping with the changes that have occurred.

### **The Impact of eHealth**

A change in the ethical framework occurred with the advent of eHealth. eHealth is the delivery of health care by health care professionals and institutional health care providers by electronic means. The previous role of HIPs in the delivery of health care both at the professional and the institutional level was that of supportive technical players in a framework that was rooted in the physician-patient encounter and whose inception was triggered and conditioned by the health care professionals' (HCPs) direct and unmediated relationship with their patients. While the work of HIPs was important and quality-enhancing, it was not existentially enabling either for the inception of the clinician-patient relationship or for the delivery of health care itself. With eHealth, this changed. Without the active involvement of HIPs the fiduciary HCP-patient relationship could never arise and the framework within which health care is delivered could not exist.

At first glance, such a claim may seem astounding, for eHealth appears to be nothing more than the application of modern communication technology to a distanced mode of health care delivery, and the use of sophisticated communication tools such as Skype<sup>3</sup> or the use of

---

<sup>3</sup>Armfield NR, Bradford M and Bradford NK. The clinical use of Skype—For which patients, with which problems and in which settings? A snapshot review of the literature. *International Journal of Medical Informatics* 84, 737-742.

electronic health records (EHRs)<sup>4</sup> and other electronic aids has become relatively standard practice in modern health care.<sup>5</sup> However, this perspective is based on too limited an understanding of the novel nature of eHealth and of the role that HIPs play in its delivery. The adoption of diagnostic, communication, and information technology in previous incarnations of health care did not alter the fiduciary fabric of health care because what had traditionally grounded its inception—the direct clinician-patient encounter—remained unchanged, and although the fabric of rights and obligation had expanded to include HIPs with the introduction of electronic records, telecommunication, etc., whatever obligations HIPs had was derivative of the primary clinician-patient grounding.

eHealth fundamentally changed this landscape. The role of HIPs changed from that of supportive technical players embedded in a framework that was rooted in the clinician-patient encounter and that was triggered by the primacy of the health care professional's (HCP's) fiduciary obligations to that of operant interface between health care institutions, clinicians, and patients, and to that of facilitators of the fiduciary relationship itself. In this facilitated encounter the digital patient record—which hitherto had been a pragmatic tool that could in principle be dispensed with<sup>6</sup>—became an integral feature not merely of the encounter itself but of the very conduct of health care; and with this the ethics that had evolved regarding patient privacy and ownership rights—to mention just two issues—transferred an obligation structure to HIPs that had previously attached mainly to HCPs and institutions. To put it bluntly, HIPs acquired a fiduciary role *sui generis* that can no longer be ignored. This new role is complicated by the confounding factor that while organizationally the delivery of eHealth assumes a unitary structure and framework as a requirement of functional possibility and operational efficiency, the pragmatic reality is that the socio-cultural and legal embedding of the various players in eHealth when it is expanded to its full potential may not be the same. It is this fact that grounds a shift in fiduciary status for HIPs and that triggers new ethical considerations.

---

<sup>4</sup>Here as elsewhere in this document, the term “Electronic Health Record” is used as a compendious expression for records that are kept on hospitals and health networks are generally called electronic health records(EHRs), electronic medical records that are kept in physicians’ offices (EMRs) as well as for personal health records (PHRs) which contain the same types of information as EHRs and EMRs but usually are less formally structured because they are designed to be accessed by the patients themselves. For a discussion of the ethics relative to such records themselves, see E-H W Kluge, “Electronic Health Records,” *Encyclopedia of Global Bioethics*, available at [http://link.springer.com/referenceworkentry/10.1007/978-3-319-05544-2\\_168-1](http://link.springer.com/referenceworkentry/10.1007/978-3-319-05544-2_168-1).

<sup>5</sup>Hsiao C-J and Hing E, Use and Characteristics of Electronic Health Record Systems Among Office-based Physician Practices: United States, 2001–2013. NCHS Data Brief 143 (January 2014); accessed 16/12/15 at <http://www.cdc.gov/nchs/data/databriefs/db143.htm>

<sup>6</sup>While many jurisdictions have implemented EHR and eHealth plans and strategies, realization of these is variable. See Gunter, Tracy D; Terry, Nicolas 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 (1): e3; Patel V, Jamoom E, Hsiao CJ, Furukawa MF, Buntin M. Variation in electronic health record adoption and readiness for meaningful use: 2008-2011, *J Gen Intern Med*. 2013 Jul;28(7):957-64; Xierali IM, Hsiao CJ, Puffer JC, Green LA, Rinaldo JC, Bazemore AW, Burke MT, Phillips RL Jr. The rise of electronic health record adoption among family physicians. *Ann Fam Med*. 2013 Jan-Feb;11(1):14-9; etc.

More specifically, someone’s instrumental, facilitating, and enabling involvement in a given enterprise triggers co-responsibility for the enterprise itself. This is not simply a matter of logic or ethics. It also finds reflection in legal pronouncements and decisions.<sup>7</sup> HIPs are integrally and instrumentally involved in the conduct of eHealth in this very sense. It therefore follows that any violation of patient privacy rights that occur in this connection will implicate HIPs because they are co-determinative of the causal flow of events that constitutes eHealth, and hence share in responsibility. This goes far beyond what was previously the case for HIPs, and deserves acknowledgement and assessment on its own terms.

Further, while providing eHealth services was initially limited to the sharing of health and patient records and was confined within national boundaries, eHealth services have since expanded to involve the actual provision of care through telemedicine and related services, and have begun to transcend national settings and to assume global parameters.<sup>8</sup> This in turn set up a new problematic for HIPs. For instance, when the eHealth providers store their EHRs in jurisdictions other than those where the service is actually delivered (cloud storage), the privacy rights of patients in the jurisdiction-of-delivery may be different from those of the jurisdiction-of-storage, and what is legal in the latter jurisdiction may not be legal in the former. 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 privacy rights that are guaranteed in the jurisdiction-of-delivery.

Likewise, when the eHealth care providers are incorporated in jurisdictions like the USA where provisions like the USA PATRIOT Act<sup>9</sup> apply to the parent institutions or corporations—and by extension are assumed to apply to their subsidiaries—the legal provisions of such Acts may provide that EHRs may be accessed by security forces of the parent institution or corporation’s jurisdiction without patient consent or knowledge. While the actions of the HIPs as facilitators and of corporate employers and service providers may be legal in the parent institution or corporation’s jurisdiction-of-incorporation, they may not necessarily be legal in the jurisdiction-of-delivery. Nor is this an idle or purely theoretical concern. The very issue lay at the heart of the case of *Maximillian Schrems v. Data Protection Commissioner*,<sup>10</sup> where the Court of Justice of the European Union explicitly took notice of this fact and ruled against the corporate

---

<sup>7</sup> *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ©-131/12), European Court of Justice, 13,5.2014; International Criminal Tribunals for the former Yugoslavia, Judgment in *Kordic* (IT-95-14/2, Appeals Chamber, 17 December 2004) §§ 24-28; and International Criminal Tribunals for Rwanda, Judgment in *Mpambara* (ICTR-01-65-T) Trial Chamber, 11 September 2006 §§ 18-20.

<sup>8</sup>For discussion of some trends and issues, see WHO *Global Observatory for eHealth* vol. 3-6.

<sup>9</sup>Public Law Pub.L. 107–56, “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”, re-enacted as Public Law 114-23 “USA Freedom Act” accessed 11/27/15 at <https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf>.

<sup>10</sup>Court of Justice of the European Union, Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner*, accessed 11/27/15 at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf>.

data organization. While the specific point at issue was not health information, there is no doubt that the principle enunciated in this judgement also applies to health information in the conduct of eHealth.

It is for these reasons that it was felt that the current IMIA *Code of Ethics of Health Information Professionals*<sup>11</sup> should undergo a careful review with the aim to ensure that it was current, and to deal with any issues that were not currently addressed. After lengthy consultation it became clear that a wholesale revision of the *Code* was not warranted since the clauses of the *Code* as presently constituted continue to adequately address the types of situations that HIPs commonly face in traditional health care; that what was needed was an expansion of the *Code* into the area of eHealth and telemedicine. This, so it seemed, could most easily be achieved by adding a separate section that addresses the ethical issues that confront HIPs when they become involved in eHealth. What follows is the result of this consultation and is an attempt to provide such an addition.

### **HIPs engaged in eHealth**

Over and above the ethical duties that HIPs incur insofar as they are active in a professional capacity in the area of health care, HIPs who are professionally active in the establishment, maintenance, and conduct of eHealth systems incur the following further obligations:

#### ***1. Obligations towards patients***

HIPs have an obligation to:

(a) take all reasonable steps to ensure that the rules, regulations, and procedural guidelines that govern the technical services of the eHealth institution or corporation with which they are professionally associated are consistent not only with patients' information rights in

(i) the eHealth provider's jurisdiction of incorporation, and in

(ii) the jurisdiction where patient data are stored, accessed, used, communicated or manipulated,

but also with patients' information rights in

(iii) the jurisdiction in which the patients receive the services that are delivered by the eHealth institution or corporation;

(b) take all reasonable steps to ensure that the eHealth institution or corporation with which they are professionally associated have effective measures in place to ensure that the patients, who are served by the eHealth institution or corporation, are aware of their information rights, and have effective means for addressing any matter that may arise in this regard; and

---

<sup>11</sup> [http://www.imia-medinfo.org/new2/pubdocs/Ethics\\_Eng.pdf](http://www.imia-medinfo.org/new2/pubdocs/Ethics_Eng.pdf).

(c) take all reasonable steps to ensure that the eHealth institution or corporation with which they are professionally associated has effective measures in place to review and, if necessary, appropriately amend the measures indicated under **1(a)-1(b)** on a regular basis to ensure that they are consistent with evolving information laws in the eHealth institution or corporation's domain of operation; and

(d) participate in a professional capacity only in those eHealth institution or corporations whose operative frameworks meet the standard enunciated in **(a)-(c)**.

## ***2. Obligations towards the eHealth institution or corporations with whom they are professionally associated***

HIPs have an obligation to:

(a) take all reasonable steps to ensure that the informatics products, tools, and devices they recommend are

- (i) suitable,
- (ii) reliable, and
- (iii) qualitatively appropriate

to allow the eHealth institution or corporation to meet its informatics obligations as indicated in clause **1**;

(b) take all reasonable steps to ensure that the informatics protocols or measures they recommend or institute are

- (I) suitable,
- (ii) reliable,
- (iii) effective, and
- (iv) qualitatively appropriate

to allow the eHealth institution or corporation to meet its informatics obligations as indicated in clause **1**;

(c) take all reasonable steps to ensure that the eHealth institution or corporation with which they are professionally associated is made aware in good time of any changes in the informatics obligations incurred by an eHealth provider in its domain of operation; and

(d) be professionally qualified and certified in keeping with the highest current professional standards to provide informatics services relevant to eHealth; and continue to be thus qualified for the duration of their professional association.

## **3. Obligations towards Health Care Professionals (HCPs)**

HIPs have an obligation to take all reasonable steps to ensure, insofar as this is possible under the circumstances, that the HCPs who depend on their informatics services:

(a) are aware of any differences in information rights that the HIPs' provision of professional services might affect the HCPs' patient-relative actions in an interjurisdictional setting insofar as this can reasonably be ascertained by the HIP;

(b) are aware of any differences in the availability of informatics tools that exist between the HCPs' location and the location of the patients with whom they interact and that are relevant to the HCPs' ability to carry out their health care mandate insofar as this can reasonably be ascertained by the HIP;

(c) are aware of any difference in qualitative standards of the informatics devices, protocols and tools that exist between the HCPs' location and the location of the patients with whom they interact and that are relevant to the HCPs' ability to carry out their health care mandate insofar as this can reasonably be ascertained by the HIP.