Incorporated under the laws of Switzerland

Ethics for Health Informatics Professionals

The IMIA Code, its Meaning and Implications

A Guide for the revised and updated *Code of Ethics for Health Informatics Professionals* that was approved August 28, 2016 by the General Council of the International Medical Informatics Association

Eike-Henner W. Kluge, PhD, FRSC

PREAMBLE

Health informatics is the discipline that deals with how health data are electronically collected, stored, manipulated, communicated and processed into health information that is suitable for administrative and clinical decision making, management, research and planning, and with how computer, information and telecommunications technologies are designed, developed and applied to support the research into and delivery of health care services. Health Informatics professionals (HIPs) are individuals who work in the area of health informatics as thus defined in a professional capacity.

Contemporary health care relies on health information for its development, planning and delivery. HIPs are therefore integrally involved in, and indeed are indispensable to, the development, planning and delivery of contemporary health care. Consequently, it is important that the conduct of HIPs be in keeping with the highest ethical standards. While ultimately this relies on the ability of HIPs to identify and apply such standards on a given occasion, the ability to do so is facilitated—and consistency of judgment in this regard is optimized—if the standards themselves are identified and stated in a code of professional ethics. The IMIA Code of Ethics for Health Informatics Professionals therefore serves several purposes: to provide ethical guidance for the professionals themselves, to furnish a set of principles against which the conduct of the professionals may be measured, and to provide the public with a clear statement of the ethical considerations that should shape the behaviour of the professionals themselves.

In this connection, it is important to note that 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 necessarily address ethical issues. Moreover, legal provisions are formulated by legislators, judges or juries with reference to current and anticipated circumstances having legal implications as these are understood at a particular point in time. Therefore, legal provisions and legal codes 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.

In contrast to these and other formal statements, codes of professional ethics are grounded in fundamental and generally accepted principles of ethics which latter, as the *Universal Declaration on Human Rights*[i] 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 ethically proceed. 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.

The Nature of and Reasons for an IMIA Code of Ethics

At the same time, it would be inappropriate for a code of ethics—and the IMIA *Code of Ethics for Health Informatics Professionals* is no exception—to try and address every possible situation that might arise. In the first place, it presupposes that it is 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 respective social embedding.

The reason for constructing a code of ethics for HIPs instead of merely adopting one of the codes that have been promulgated by the various general associations of informatics professionals[ii] is that HIPs play a unique role in the planning, development and delivery of health care: a role that, because of their domain of operation, is distinct from the role of other informatics professionals who work in different settings.

Part of this distinctness is centred in the special relationship between the electronic health record (EHR) and the subject of that record.[iii] EHRs not only reveal much about patients that is private and should be kept confidential, they also function as the bases of clinical decisions that have a profound impact on patient welfare. Furthermore, the data that are contained in EHRs also provide the raw materials for decision-making by health care institutions, governments and other agencies without which systems of health care delivery simply cannot be designed, developed or function. Moreover, EHRs provide the data that are used by duly empowered researchers to analyze and evaluate various aspects of current health care delivery, to improve or modify the latter, and to develop both new practices as well as new tools such as pharmaceuticals, surgical and medical techniques and the like. Since HIPs play a fundamental role in the construction, maintenance, storage and communication of EHRs, and because of the role the latter and their communication play in modern health care delivery, HIPs are subject to ethical constraints that do not necessarily hold for other informatics professionals.

Over and above the ethical constraints that arise from the relationship between EHRs and patients, the ethical conduct of HIPs is also subject to considerations that arise out of the HIPs' interactions with Health Care Professionals (HCPs), health care institutions and other agencies with whom they are associated and whose operations they facilitate. These constraints may pull in different directions. It is therefore important that HIPs have some idea of how to resolve in an appropriate fashion the ethical issues that arise in such cases. A Code of Ethics for HIPs provides a tool in this regard, and may be of use in effecting a resolution when distinct roles and constraints collide.

The Impact of eHealth and Related Matters

Of course the relevance and importance of ethical considerations for HIPs has long been recognized since it was clear from the beginning that the development and use not merely of EHRs but also of electronically assisted diagnostic devices and health care delivery systems imposes special obligations on HIPs: obligations that go beyond the need for technical proficiency in providing security, usability and accessibility of the EHRs themselves or of the functionality of the various devices used in developing,

gathering and interpreting the data that had become the tool-in-trade of modern health care professionals and of health care administrators, researchers and corporations. It also includes, insofar as this lies within the capabilities of HIPs, the development and maintenance of a security culture and of an organisational awareness of the ethical concerns relative to the development and handling of patient information.

The advent of eHealth in its various forms extended this ethical framework for HIPs. 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' 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 physician-patient relationship itself or for the delivery of health care as such. With eHealth, however, this changed. Without the active involvement of HIPs the fiduciary HCP-patient relationship could never arise and without their ongoing facilitating role the framework within which eHealth is delivered could not exist.

Such a claim may seem astounding, for at first glance eHealth appears to be nothing more than the application of modern communication technologies to a distanced mode of health care delivery and the use of sophisticated communication tools such as Skype[iv] and cell-phones, or the use of electronic health records (EHRs)[v] and other electronic means and devices. However, closer consideration shows that 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 physician-patient encounter—remained unchanged; and although the fabric of rights and obligation had expanded to include HIPs with the introduction of electronic health records, telecommunication etc., whatever obligations HIPs had was derivative of the physician-patient relationship which grounded the whole framework.

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 physician-patient encounter and that was triggered by the primacy of the health care professional's (HCP's) fiduciary obligations to that of operant interfaces between health care institutions,[vi] physicians 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[vii]— became an integral feature not merely of the encounter itself but of the very conduct of health care. With this, the ethics that had evolved regarding patient privacy and ownership rights—to mention just two issues—transferred obligations to HIPs that had previously attached mainly to HCPs and institutions. To put it bluntly, HIPs acquired a fiduciary role *sui generis* that could no longer be ignored. This new role is complicated by the confounding factor that while organisationally 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 unitary at all but extend over several domains. It is these facts that entail a shift in fiduciary status for HIPs and that trigger the new ethical considerations that are identified in the revised IMIA Code of Ethics as ratified and approved in 2016.[viii]

The key fact here is that 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.[ix] HIPs are integrally and instrumentally involved in the conduct of eHealth in this very sense. It therefore follows that any violation of patient privacy and related informatic rights that occurs in this connection will implicate HIPs because they are co-determinative of the causal flow of events that constitutes eHealth. Hence they 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.[x] This, in turn, sets 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 (e.g., 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, to the best of their ability, 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 or organizations that provide informatic services to health care providers that are incorporated in jurisdictions like the USA, where provisions like the USA PATRIOT Act[xi] or legal provisions like it are in force, such providers or organizations—and by extension their subsidiaries—may be required to produce or provide access to any EHR that is held by them or under their control without patient knowledge or consent. While the actions of the HIPs as facilitators and of health care service providers, institutions or organizations who meet such a request may be legal in their jurisdiction-of-incorporation, they may not necessarily be legal in the jurisdiction-of-service-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*,[xii] where the Court of Justice of the European Union explicitly took notice of this fact and ruled against the corporate 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.

The Code Revision and Revised Handbook

It is for these reasons that it was felt that the IMIA Code of Ethics for Health Informatics Professionals that had been endorsed on October 4, 2002 in Taipei required a careful review with the aim to ensure that it was current, and to deal with any issues that were not being addressed.

After lengthy and extensive consultation, it became clear that despite the fundamental changes that had occurred in the professional role of HIPs engaged in eHealth, a wholesale revision of the Code was not warranted since the clauses of the Code as endorsed in 2002 continue to adequately address the types of situations that HIPs commonly face in traditional health care. What was needed was an expansion of the Code into the area of eHealth, mHealth and telemedicine. This, so it was felt, could most easily be achieved by adding distinct clauses to the old Code so as to address the ethical issues that confront HIPs when they become involved in eHealth and similar undertakings. Not surprisingly, therefore, the revised Handbook overlaps to a considerable extent with the Handbook as previously developed. Editorial changes aside—and there have been some in order to improve its readability—the distinctive feature of the new Handbook is the addition of discussions that deal with the changes that have been made to the original Code. In particular, this includes discussions of the revisions to Section A: *Subject-centred Duties*, Section B: *Duties towards HCPs*, Section C: *Duties towards Institutions, Employers and Agencies*, and Section D: *Duties towards Society*.

For the sake of explanatory clarity this Handbook is divided into two parts. **Part I** contains the overall ethical framework that should guide the actions of HIPs in their professional lives. It consists of a brief sketch of *Fundamental Principles of Ethics* that have found general global acceptance. Next is a brief list of general *Principles of Informatic Ethics*, which follow from these fundamental ethical principles when these are applied to the informatic setting. This in turn is followed by the *IMIA Code of Ethics for Health Informatics Professionals*, which identifies the ethical rules of conduct that HIPS should follow in their professional lives. The Code itself is updated as of August 28, 2016. **Part II** consists of *Explanations* for the various provisions that are contained in the updated Code. As with the previous version of this Handbook, its purpose is to provide some guidance for interpreting and applying to actual situations the rules of conduct that make up the IMIA Code of Ethics.

Part I.

Introduction

Fundamental Principles of Ethics

All social interactions are subject to fundamental ethical principles. HIPs function in a social setting. Their actions, therefore, are also subject to these principles. The most important of these principles are:

1. *Principle of Autonomy*

> All persons have a fundamental right to self-determination.[xiii]

2. *Principle of Equality and Justice*

> All persons are equal as persons and have a right to be treated accordingly.[xiv]

3. *Principle of Beneficence*

> All persons have a duty to advance the good of others where the nature of this good is in keeping with the fundamental and ethically defensible values of the affected party.[xv]

4. *Principle of Non-Malfeasance*

> All persons have a duty to prevent harm to other persons insofar as it lies within their power to do so without undue harm to themselves.[xvi]

5. *Principle of Impossibility*

> All rights and duties hold subject to the condition that it is possible to meet them under the circumstances that obtain.[xvii]

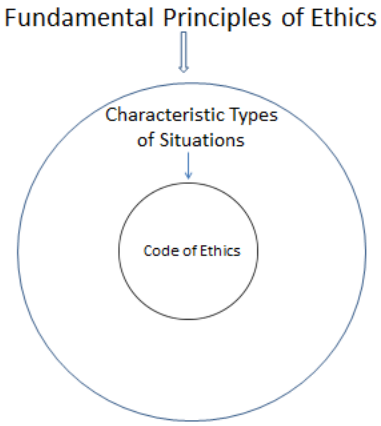
6. *Principle of Integrity*

> Whoever has an obligation has a corresponding duty to fulfil that obligation to the best of her or his ability.[xviii]

General Principles of Informatic Ethics

These Fundamental Principles of Ethics, when applied to a particular type of setting, give rise to more particularized versions that lay out the ethical landscape of that area in more specific terms, where these

latter may be collected together into a Code of Ethics for the professionals who work in that type of setting. This relationship may be represented diagrammatically as follows:



These considerations, therefore, underlie the derivation of the General Principles of Informatic Ethics. There are seven such Principles: the Principle of Information-Privacy and Disposition, the Principle of Openness, the Principle of Security, the Principle of Access, the Principle of Legitimate Infringement, the Principle of the Least Intrusive Alternative, and the Principle of Accountability.

1. *Principle of Information-Privacy and Disposition*

All persons have a fundamental right to privacy, and hence to control over the collection, storage, access, use, communication, manipulation and disposition of data about themselves.

2. *Principle of Openness*

The collection, storage, access, use, communication, manipulation and disposition of personal data must be disclosed in an appropriate and timely fashion to the subject of those data.

3. *Principle of Security*

Data that have been legitimately collected about a person should be protected by all reasonable and appropriate measures against loss, degradation, unauthorized destruction, access, use, manipulation, modification or communication.

4. *Principle of Access*

The subject of a health record has the right of access to that record and the right to correct the record with respect to its accurateness, completeness and relevance.

5. *Principle of Legitimate Infringement*

The fundamental right of control over the collection, storage, access, use, manipulation, communication and disposition of personal data is conditioned only by the legitimate, appropriate and relevant data-needs of a free, responsible and democratic society, and by the equal and competing rights of other persons.

6. *Principle of the Least Intrusive Alternative*

Any infringement of the privacy rights of the individual person, and of the individual's right to control over person-relative data as mandated under Principle 1, may only occur in the least intrusive fashion and with a minimum of interference with the rights of the affected person.

7. *Principle of Accountability*

Any infringement of the privacy rights of the individual person, and of the right to control over person-relative data, must be justified to the affected person in good time and in an appropriate fashion.

As was said, these General Principles of Informatic Ethics derive from the application of the Fundamental Principles of Ethics to the types of activities in which HIPs characteristically engage or which they facilitate in their professional capacity, as well as to the relationships into which they enter in their professional lives and to the types of situations that they encounter when thus engaged. The *Code of Ethics for Health Informatics Professionals* outlines the more important particular ethical duties and rights that derive from these Principles of Informatic Ethics. It should be noted that as with any code of ethical conduct, the Code itself cannot do more than provide guidance. The precise way in which the various clauses of the Code apply in a given context, and the precise nature of particular ethical rights or obligations that are involved, depends on the specific nature of the relevant situation. While the various clauses themselves merely identify the ethically relevant considerations that should guide the behaviour of HIPs, the section entitled *Explanations* outlines the reasoning that underlies the various clauses and provides clarification of why and how they relate to the General Principles of Informatic Ethics and their implication for HIPs.

The IMIA Code of Ethics for Health Informatics Professionals (2016)

A. Subject-centred Duties

These are duties that derive from the relationship between electronic health records, the data that are contained in them and the subjects of those records. These duties arise from the fact that HIPs are instrumental in their construction, maintenance, storage, linkage, use, manipulation and communication.

1. HIPs have a duty to ensure that the potential subjects of electronic health records are made aware of the existence of systems, programmes, protocols or devices whose purpose is to collect and/or communicate data about them.

2. HIPs have a duty to ensure that appropriate procedures are in place so that

> **a.** electronic health records are established, maintained, stored, used, linked, manipulated or communicated only with the voluntary, competent and informed consent of the subjects of such records, and
>
> **b**. the subjects of electronic health records are informed of any contravention of **A.2.a** in good time and in an appropriate fashion.

3. HIPs have a duty to ensure that the subjects of electronic health records are made aware of

> **a**. who has established them and who maintains them,
>
> **b.** what is contained in them,
>
> **c.** the purpose for which they are established,
>
> **d.** the individuals, institutions or agencies who have access to them or to whom they (or identifiable parts thereof) may be communicated,
>
> **e.** where the records are maintained,
>
> **f**. the length of time they will be maintained, and
>
> **g**. the ultimate nature of their disposition.

4. HIPs have a duty to ensure that the subjects of electronic health records are made aware of the origin of the data contained in their records.

5. HIPs have a duty to ensure that the subjects of electronic health records are made aware of any rights they may have with respect to

> **a**. access, use and storage,

b. communication, linkage and manipulation,

c. quality and correction, and

d. disposition

of their electronic health records and of the data contained in them.

6. HIPs have a duty to ensure that

a. electronic health records are stored, accessed, used, linked, manipulated or communicated only for legitimate purposes;

b. there are appropriate protocols and mechanisms in place to monitor the storage, access, use, linkage, manipulation or communication of electronic health records, or of the data contained in them, in accordance with section **A.6.a**;

c. there are appropriating protocols and mechanisms in place to act on the basis of the information under section **A.6.b** as and when the occasion demands;

d. the existence of these protocols and mechanisms is made known to the subjects of the records; and

e. there are appropriate means for subjects of the records to enquire into and to engage the relevant review protocols and mechanisms.

7. HIPs have a duty to treat the duly empowered representatives of the subjects of electronic health records as though they had the same rights concerning the records as the subjects of the records themselves, and that the duly empowered representatives (and, if appropriate, the subjects of the records themselves) are made aware of this fact.

8. HIPs have a duty to ensure that all electronic health records are treated in a just, fair and equitable fashion.

9. HIPs have a duty to ensure that all reasonable and appropriate measures are in place that may reasonably be expected to safeguard the

a. security,

b. integrity,

c. material quality,

d. usability, and

e. accessibility

of electronic health records.

10. HIPs have a duty to ensure, insofar as this lies within their power, that electronic health records and the data contained in them are used only

a. for the stated purposes for which the data were collected, or

b. for purposes that are otherwise ethically defensible.

11. HIPs who are professionally involved in the establishment, maintenance or conduct of eHealth have an obligation

a. to take all reasonable steps to ensure that the rules, regulations and procedural guidelines that govern the informatic practices and services of the eHealth providers with whom they are professionally associated are consistent with the informatic rights of the subjects of electronic health records in

i. the eHealth providers' jurisdiction of incorporation,

ii. the jurisdiction where the records are stored, accessed, used, linked, manipulated or communicated by the eHealth providers, and

iii. the jurisdiction in which the subjects of the records receive the services that are delivered by the eHealth providers;

b. to take all reasonable steps to ensure that the eHealth providers with whom they are professionally associated have effective measures in place to ensure that the individuals who are served by the eHealth providers are aware of their informatic rights, and have effective means in place for addressing any disputes or matters that may arise in this regard;

c. to take all reasonable steps to ensure that the eHealth providers with whom they are professionally associated have effective measures in place to review and, if necessary, to appropriately amend the measures indicated under **11(a)-11(b)** on a regular basis in order to ensure that they are consistent with evolving informatic standards and laws in the eHealth providers' domains of operation; and

d. to engage in a professional capacity only with those eHealth providers whose operative frameworks[xix] meet the standard enunciated in **11(a)-11(c)**.

12. HIPs have a duty to ensure that the subjects of electronic health records are made aware in good time and in an appropriate fashion of possible breaches of the preceding duties and the reason for such breaches.

B. Duties towards Health Care Professionals (HCPs)

HCPs who care for patients depend on the services of HIPs for the fulfilment of their patient-centred obligations. Consequently, HIPs have an obligation to assist the HCPs with whom they are associated in a professional capacity insofar as this is compatible with the HIPs' primary duty towards the subjects of the electronic health records. Specifically, this means that

1. HIPs have a duty

> **a**. to assist duly empowered HCPs who are engaged in patient care or planning in having appropriate, timely and secure access to relevant electronic health records (or parts thereof), and to ensure the usability, integrity, and highest possible technical quality of these records; and
>
> **b.** to provide those informatic services on which the HCPs rely to carry out their mandate.

2. HIPs should keep HCPs informed of the status of the informatic services on which the HCPs rely, and immediately advise them of any problems or difficulties that might be associated with or that could reasonably be expected to arise in connection with these informatic services.

3. HIPs have an obligation to take all reasonable steps to ensure that HCPs who are engaged in eHealth and who depend on the HIPs' informatic services

> **a.** are made aware of any differences in informatic rights or standards that might affect the HCPs' ability to carry out their mandate in the relevant interjurisdictional settings;
>
> **b.** are made aware of any differences in the availability of informatic devices, protocols, tools etc. 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; and
>
> **c.** are made aware of any difference in qualitative standards of the informatic devices, protocols, tools etc. 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.

4. HIPs should advise the HCPs with whom they interact on a professional basis or for whom they provide professional services of any circumstances that might prejudice the objectivity of the advice they give or that might impair the nature or quality of the services that they perform for the HCPs.

5. HIPs have a general duty to foster an environment that is conducive to the maintenance of the highest possible ethical and material standards of data collection, storage, management, communication and use by HCPs within the health care setting.

6. HCPs who are directly involved in the construction of electronic health records may have an intellectual property right in certain formal features of these records. Consequently, HIPs have a duty to safeguard

> **a.** those formal features of the electronic health record, or
>
> **b.** those formal features of the data collection, retrieval, storage or usage system in which the electronic health record is embedded

in which the HCPs have, or may reasonably be expected to have, an intellectual property interest.

C. Duties towards Institutions, Employers and Agencies

1. HIPs owe the institutions, employers or agencies with whom they are professionally associated a duty of

a. competence,

b. diligence,

c. integrity, and

d. loyalty.

2. HIPs have a duty

a. to take all reasonable steps to ensure that the informatic products, services, tools or devices they recommend to the institutions, employers or agencies with whom they are associated in a professional capacity are

(i) suitable,

(ii) reliable,

(iii) effective, and

(iv) qualitatively appropriate

so as to allow the latter to meet their respective obligations;

b. to take all reasonable steps to ensure that the informatic protocols or procedures they recommend or institute are

(i) suitable,

(ii) reliable,

(iii) effective, and

(iv) qualitatively appropriate

to allow the institutions, employers or agencies with whom they are associated in a professional capacity to meet their relevant obligations;

c. to take all reasonable steps to ensure that the institutions, employers or agencies with whom they are associated in a professional capacity are made aware in good time and in an appropriate fashion of any differences in the informatic obligations that may reasonably be expected to affect the latter's operation in an eHealth context or in an interjurisdictional domain of operation;

d. to take all reasonable steps to ensure that the institutions, employers or agencies with whom they are associated in a professional capacity are made aware in good time and in an appropriate fashion of any differences in the material and technical resources that may reasonably be expected to affect the latter's' operation in an eHealth context or in an interjurisdictional domain of operation;

e. to be professionally qualified and certified, and to continue to be qualified and certified, in keeping with the highest current professional standards in the institutions', employers' or agencies' domains of operation.

3. HIPs have a duty to

a. foster an ethically sensitive security culture in the setting in which they practice their profession,

b. facilitate the planning and implementation of the best and most appropriate data security measures possible for the setting in which they work, and

c. implement and maintain the highest possible qualitative and ethical standards of data collection, storage, retrieval, processing, accessing, communication, linkage and utilization in all areas of their professional endeavour.

4. HIPs have a duty to ensure, to the best of their ability, that appropriate measures are in place to evaluate the technical, legal and ethical acceptability of the data-collection, storage, retrieval, processing, accessing, communication, linkage and utilization of data in the settings in which they carry out their work or with which they are affiliated.

5. HIPs have a duty to alert, in good time and in a suitable manner, appropriately placed decision-makers of the security- and quality-status of the data-generating, storing, accessing, handling, linking and communication systems, programmes, devices or procedures of the institutions with whom they are affiliated or of the employers for whom they provide professional services.

6. HIPs should immediately inform the institutions, employers or agencies with whom they are affiliated or for whom they provide professional services of any problems or difficulties that could reasonably be expected to arise in connection with the performance of their contractually stipulated services.

7. HIPs should immediately inform the institutions, employers or agencies with whom they are affiliated or for whom they provide professional services of circumstances that might prejudice the objectivity of the advice they give.

8. Except in emergencies, HIPs should only provide services in their areas of competence, and should always be honest and forthright about their education, experience, qualification and training.

9. HIPs should only use suitable and ethically acquired or developed tools, protocols, techniques, programmes or devices in the execution of their duties.

10. HIPs have a duty to assist in the development and provision of appropriate informatics-oriented educational services in the institutions or agencies with whom they are professionally affiliated or for the employers for whom they work.

D. Duties towards Society

1. HIPs have a duty to facilitate the appropriate

a. collection,

b. storage,

c. communication,

d. use,

e. linkage and

f. manipulation

of health care data that are legitimately used in research or that are necessary for the planning and providing of health care services on a social scale.

2. HIPs have a duty to ensure, insofar as this falls within their area of competence, that

a. only data that are relevant to legitimate research or planning needs are collected;

b. the data that are collected are de-identified or rendered anonymous as much as possible, in keeping with the legitimate aims of the collection;

c. the linkage of data bases can occur only for otherwise legitimate and defensible reasons that do not violate the fundamental rights of the subjects of the records; and

d. only duly authorised persons have access to the relevant data.

3. HIPs have a duty to educate the public about the various issues associated with the nature, collection, storage, use, linkage and manipulation of health related data and to make society aware of any problems, dangers, implications or limitations that might reasonably be associated with the collection, storage, use, linkage and manipulation of such data.

4. HIPs will refuse to participate in or support practices that violate human rights.

5. HIPs will be responsible in setting the fee for their services and in their demands for working conditions, benefits, etc.

E. Self-regarding Duties

1. HIPs have a duty to recognize the limits of their competence.

2. HIPs have a duty to consult when necessary or appropriate.

3. HIPs have a duty to maintain competence.

4. HIPs have a duty to take responsibility for all actions performed by them or under their control or authority.

5. HIPs have a duty to avoid conflict of interest.

6. HIPs have a duty to give appropriate credit for work done.

7. HIPs have a duty to act `with honesty, integrity and diligence.

F. Duties towards the Profession

1. HIPs have a duty to always act in such a fashion as not to bring the profession into disrepute.

2. HIPs have a duty to assist in the development of the highest possible standards of professional competence, to ensure that these standards are publicly known, and to see that they are applied in an impartial and transparent manner.

3. HIPs will refrain from impugning the reputation of colleagues but will report to the appropriate authority any unprofessional conduct by a colleague.

4. HIPs have a duty to assist their colleagues in living up to the highest technical and ethical standards of the profession.

5. HIPs have a duty to promote the understanding, appropriate utilization, and ethical use of health information protocols and technologies, and to advance and further the discipline of Health Informatics.

Part II

Discussion and Explanations

This section of the Handbook provides detailed explanations of the ethical reasoning that underlies the various clauses of the *Code of Ethics for Health Informatics Professionals*. Its purpose is to give some insight into the basis of the various clauses, what they mean and how they should be interpreted. Its purpose, therefore, is to assist HIPs in understanding the implications of the various clauses contained in the *Code* and in applying the *General Principles of Informatic Ethics* to situations that are not specifically dealt with in the *Code* itself.

When considering what follows, it should also be recalled that the *Code of Ethics* does not include what might be called 'technical' provisions. That is to say, it does not specify such things as technical standards for secure data communication or provisions that are necessary to ensure a high quality in the handling, collecting, storing, transmitting, manipulating, etc. of health care data. This is deliberate. While the development and implementation of technical standards has ethical dimensions, and while these dimensions are reflected in the *Code*, the details of such technical standards are not themselves a matter of ethics. For this reason, the discussions and explanations that follow make no reference to specific technical provisions except insofar as it is an ethical obligation of HIPs to ensure, to the best of their ability, that relevant and appropriate technical standards are met. HIPs who seek information in this regard are referred to the relevant ISO standards[xx] as well as to the technically oriented proficiency provisions of their respective countries and domains of operation.

A. Subject-centred Duties

Introduction

The purpose of this section is to give a more detailed explanation of the subject-centred duties of HIPs. However, before actually doing so, it is important to clarify what is meant by saying that the health informatics specialist is a professional. The reason this is important is that the ethical considerations that are relevant for professionals are different from those that apply to individuals who are merely employees. Specifically, a professional's obligations are fiduciary in nature and are owed to the individual who is the recipient of the professional's services even when this recipient is not the one who pays for the services in question. While the precise legal nature and extent of a fiduciary duty may vary from jurisdiction to jurisdiction, ethically speaking it is generally agreed that a professional's fiduciary obligations go beyond merely doing what is explicitly stated in the agreement that forms the basis of the professional's actions. They extend to doing what is in the best interests of the individual who is the recipient or subject of the professional's action even when there are no specific contractual directives in this regard.

By contrast, the obligations of an employee are purely contractual in nature, and are wholly and completely circumscribed by the clauses of the contract itself. Further, the obligations of an employee in an institutional setting directly extend only towards the employer; they extend towards the client only indirectly through the primary obligation that the institution owes towards its clients. Consequently, considerations of best interests relative to the recipient or subject of the employee's action enter the picture only indirectly, if at all.

Health Informatics specialists are professionals even when they are in the employ of an institution or corporate entity. This follows from the definition of a profession itself.

That is to say, in sociological terms, a profession is characterized by several features, most of which are shared by all professions. For example, the work that the members of a profession perform usually has a significant intellectual component and has an impact not only on their clients but also on the welfare of society. As well, members of a profession usually have undergone a specialized form of education, frequently at the post-secondary or university level, and membership may require a certification or accreditation of proficiency and expertise where the nature and level of this is frequently determined by the group itself. Moreover, a profession may also be accorded the right of self-governance, and may be granted a legally recognized practice monopoly or exclusivity of practice. In that eventuality, only individuals who are licensed and have been certified to meet the standards that have been promulgated by the profession may engage in the activities in question. Finally, professions are often organized into associations or groups of associations that represent the profession to society, and the conduct of a profession's members is often governed by a more or less formalized set of rules or a code of conduct, where infringement of the latter may result in the loss of the licence to practice and even to legal action. [xxi]

It is not necessary that a profession exhibit all of these characteristics. Thus, legal recognition and exclusivity of practice are matters of law and depend on the legal framework in which the profession functions. Therefore, whether a given profession enjoys this status depends on the national legal framework within which it operates. For example medicine, which is a paradigm of a profession, did not attain legal recognition and exclusivity of practice until the turn of the twentieth century and other individuals such as barber surgeons, midwives, herbalists, nuns, priests, shamans etc. were at liberty to provide medical services.[xxii] Likewise, nursing services were originally provided by individuals who had not necessarily undergone a formalized programme of training and has been recognized as a profession only since the turn of the twentieth century.[xxiii] Even now there are jurisdictions in which nursing does not enjoy a legally recognized service provider monopoly, and individuals who essentially have only lay standing may function in what in other countries is a professional nursing capacity as nurses.[xxiv]

On the other hand, advanced and specialized education has been a universal characteristic of all professions, even historically. Thus, lawyers and members of the medical profession were expected to have advanced education even in the Middle Ages – an expectation that was (briefly) translated into a matter of law in the 13th century [xxv] and re-instituted in the 20th. Health Informatics shares this characteristic. Health Informatics specialists, in order to function in a professional capacity, usually require advanced, formalised and special education—usually at the post-secondary or university level.

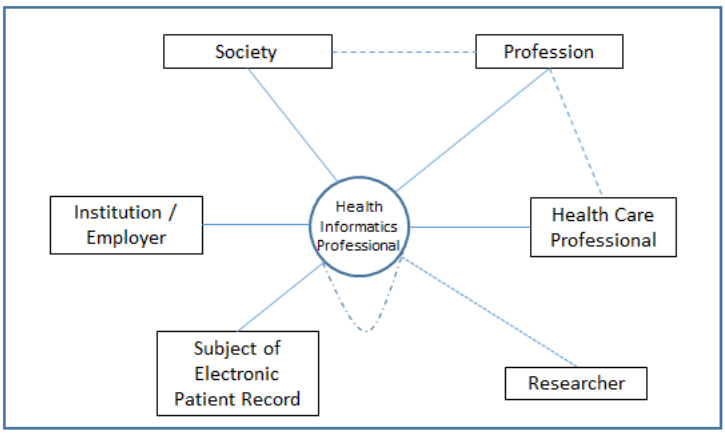
As well, Health Informatics has in common with other professions that it provides a socially important service. Moreover, it also shares the characteristic that its members are frequently organized into associations that impose rules of conduct on their members.[xxvi]

Fiduciary nature of the HIP–patient relationship

As was said before, HIPs stand in a fiduciary relationship towards the individuals who are the subjects of their services as well as towards their employers and the health care professionals who rely on their services. The reason for this lies in the fact that HIPs are at the at the centre of a web of interlocking relationships between the subject of the electronic health record and a series of interested parties whose endeavours focus on the welfare of patients and who all share a need for patient-related information. These other parties include the HCPs who provide patient care, the institutions or agencies that employ the HIPs, insurance companies, governmental agencies that gather data for health care planning purposes, and managers who are responsible for the administrative structures within which health care is delivered, etc. The reason HIPs occupy this unique position is that neither HCPs nor anyone else can function without the data that are contained in the electronic health record, and it is the HIPs who provide the necessary technical expertise that makes the development, access, use, manipulation and communication, etc. of these data possible.

It may be helpful to briefly sketch the web of the major ethical relationships in which HIPs are embedded:

Ethical Embedding of Health Informatics Professionals



In this web of relationships, the relationship between the HIP and the subject of the electronic health record is the most important. The reason for this lies in the unique connection between the electronic health record and the subject of the record, as well as the in the role that the record plays in the delivery of modern health care. Not only does the record contain sensitive data that the subject reveals or

otherwise makes available only on the understanding of confidentiality, it also plays a crucial role in the delivery of health care to the subject. Therefore, not only is *privacy* an overwhelming concern, but so are *availability,* which is to say that he record must be available when it is needed; *quality,* which means that the record must be materially usable by whoever provides the relevant health care; *security*, which means that the record must not have been accessed or altered in an unauthorized fashion or by an unauthorized person; and *usability*, which means that the record must be in such an electronic form that it can actually be retrieved and used by the current software programs of the duly authorized and authenticated users. Unless the health informatics specialist acts in a professional manner, none of this will be possible.

Trust

When patients enter the modern health care setting they trust that the framework into which they enter will deal with their health care needs in an appropriate fashion. The overt focus of that trust are the health care professionals with whom they interact and, to a lesser degree, the administrators who are responsible for administrative aspects of the framework in which the health care is delivered.

However, in fact the patients also enter into a trust relationship with HIPs. To understand why and how this case, it may be useful to recall that the ability of HCPs to provide appropriate health care is dependent on data about the patient and on the ability to communicate with other health care professionals as and when this becomes necessary—which, in turn, is dependent on the existence and proper functioning of a technical informatic framework because without it this could not occur. It is HIPs who underwrite all of this through their professional actions. Therefore while the overt focus of the trust that patients carry with them when they enter the modern health care setting centres in the HCPs who provide hands-on care, and more distantly in administrators who are responsible for the operations of the setting as a whole, their trust unconsciously includes the HIPs who make all of this possible. With due alteration of detail, similar considerations apply to the protocols that govern the functioning of the system. HIPs are responsible for the appropriateness and effectiveness of the protocols that are employed so that data can be gathered, manipulated, communicated, stored, etc. and health care can be provided.

But more is involved than only trust in the technical aspects of the informatic structure and the technical protocols that govern its usage. Patients also trust that the data that are gathered about them will be gathered in an ethically appropriate manner, and that they will be available in good time, to appropriate persons and in usable form as and when they are needed. Further, patients also trust that the data will be secure from unauthorized access, deletion, modification, manipulation, etc. In the institutional or organisational setting in which the modern health care is typically provided, this trust can be satisfied only partially by the HCPs, administrators or other relevant persons. HIPs, by paying careful attention the ethical usage of the technology that they supply and underwrite, play a pivotal role in ensuring that the informatic right of patients are safeguarded and not infringed. The trust is implicit, to be sure, rather than explicit. In fact, most patients are not even aware of the existence of HIPs or their role in the delivery of health care; and in most cases patients will not have entered into a direct and personal relationship with the HIPs who are instrumentally involved in the delivery of their care. Nevertheless, because HIPs play a pivotal role in the modern health care setting, patients in fact place their trust in the HIPs' ethical and professional actions. The trust relationship is mediated and not direct and may not even be conscious, but it is there.

Moreover, the relationship between HIPs and patients is fiduciary in nature. The situation here is no different from the one that comes into being when a specialist consultant in a particular area of health care—say, in radiology—is consulted by the primary care physician or by the patient's health care team on a particularly complex issue. When the consultant offers an opinion as to how the care of the patient should proceed, the fact that the consulting specialist may never have met the patient—and, indeed, may never interact with the patient on a direct and personal level—does not diminish the fiduciary nature of the relationship between the consulting specialist and the patient. The patient's trust, although mediated through the person of the primary care taker and not overt, and even though generally not explicit, is still there and is still warranted. It is precisely because there is this element of trust that the patient may accuse a consultant of breach of trust if the professional does not act in a fiduciary fashion. With due alteration of detail, the same considerations apply to the relationship between the HIP and the patient.

Institutional or Organisational Expectations

Moreover, the modern institutional or organisational health care setting is structured in such a way that each professional plays a particular role in the functioning of the system as a whole. The patient may not know anything about how the system functions; nevertheless, the patient approaches the health care setting with the expectation that however it may be structured, the setting as a whole will provide appropriate services in good time, and that it will keep personal patient information private and secure. In functional terms, the institution delegates this trust to its employees or associates who actually carry out the work of the institution. Therefore, while the patient's trust may be explicitly and overtly directed towards the institution, the fact remains that, through the institution's structures and mechanisms, it devolves to the professionals who work within that institutional setting. This holds even when the institutional or organisational setting is not structured in a corporate sense such as hospitals and clinics but extends to community health systems or individualized medical or health care practice.

To repeat, the work of HIPs is integral to the operation of the health care setting itself because it is through the agency of the HIPs that the informatic needs of the institution as well as those of the HCPs who work in the institution are met. It is in the fulfilment of their professional role that the HIPs' fiduciary duty towards patients arises: it grows out the functioning of the HIPs in relation to the unique nature of electronic health record in the institutional or organisational setting.

This fiduciary relationship expresses itself in a series of duties that HIPs incur as agents of the institution. This may occur even when patient are unaware of this fact or are not in a position to determine whether some record-related issue having ethical implications, such as decision about storage, manipulation, access etc. has to be made. In fact, this will usually be the case since most of the informatically relevant actions in a health care institution go on behind the scenes. HIPs must here use their best professional judgement about how to proceed. In deciding on how to proceed, they must follow the same pattern as do other professionals who are in fiduciary relationships. This means that they must be guided either by the values of the subject of the record if these are known[xxvii] or when these are not known (which is usually the case) by the values of the objective reasonable person in the patient's position.

Moreover, it follows from the fiduciary nature of this relationship that there may be occasions when HIPs have a moral duty to engage suitable legal machinery in order to ensure that data contained in the EHR—and indeed the EHR itself—are dealt with in an ethically appropriate manner. For example, this would be the case when an informatics professional has reasonable grounds to suppose that a particular informatic undertaking is ethically inappropriate, the professional has exhausted all internal avenues for dealing with such issues and no other option remains. Furthermore, HIPs must do so irrespective of whether this means challenging a health care professional, the institution in which the informatics professional works, or the patient's significant others or next-of-kin.

It is also important to note that the HIP's domain of operation should not necessarily to be identified with the spatial setting in which the HIP works. In fact, identifying it in this way may be dangerous. It would ignore the fact that what is important about the domain of operation of a professional is not the material/physical place in which the actions of the professionals take place but the functional structure of the setting in which the professionals carry out their task. As soon as this functional structure involves the activities of the professional as professional, it is a professional setting.

In general terms, then, the relationship between a professional and a client is triggered when the would-be client enters into the domain of operation of the professional and interfaces with the more or less formalized functioning of the professional in that setting. In more particular terms that are specific to the HIP–patient relationship, this means that the HIP's domain of operation in the institutional or organisational setting is the general informatic framework of the institution as a whole. It includes the totality of computers, diagnostic machinery, wiring, programs, processes, procedures inclusive of any embedded technologies and emergent ambient assistive technologies, etc. that form the basis of the data-gathering, handling and communication capacity of the 'institution' within which the various operations of the institution are carried out.

It is in this framework that the data that form the basis of the information contained in the various records of the institution (inclusive of the electronic health record) are generated and manipulated. As was said, this means that, as soon as the patient enters into or interfaces with an institutional or organisational structure in this extended sense inclusive of the community and non-hospital setting, the fiduciary relationship between the HIP who is employed by the institution and the patient is triggered.

Procedural Implications

The fiduciary nature of the HIP–patient relationship also has other implications: implications that go beyond issues that immediately and directly concern an electronic health record on a given occasion. Some of these implications are procedural in nature. For instance, HIPs have a duty to ensure, as best as they are able, that appropriate and effective procedures, protocols and structures are in place to ensure that electronic health records will be available, in usable form, to duly authorized persons who have been authenticated as proper recipients of the records; that there are appropriate means for developing patient-relative data in keeping with the mandate of the duly accredited HCPs or institutions; that there are not only technical but also appropriate human safeguards to protect the privacy, security, integrity, material quality, etc. of the electronic health record, and so on. These duties hold for HIPs even if the institutions in which they work have no methods or procedures in place to deal with these matters. In

fact, part of the fiduciary duty of HIPs is to initiate the development and deployment of relevant, appropriate and effective measures precisely when the institutions lack such measures. Moreover, HIPs should take appropriate steps to ensure that these measures are monitored and evaluated on an ongoing basis and, if necessary, adjusted to meet changing needs.

A. Subject-centred Duties

The various duties that were indicated above derive from the fiduciary relationship in which HIP stand to the subject of the electronic health record or to the subject of the electronic communication that is facilitated by the HIPs through their professional actions.[xxviii] What follows is intended to explain the nature and implications of the various clauses that are identified in the first section of the *Code of Ethics for Health Informatics Professionals*. By way of general preamble, it should be noted that, with due alteration of detail, the explanations that follow also apply to the relationship between HIPs and the duly empowered substitute decision makers of patients who are mentally challenged, incompetent or lack capacity.

1. ***HIPs have a duty to ensure that the potential subjects of electronic health records are made aware of the existence of systems, programmes or devices whose purpose it is to collect and/or communicate data about them.***

The *Principle of Information Privacy and Disposition* provides that everyone has a right to privacy and, more particularly, of control over the collection, storage, access, use, communication, manipulation and disposition of data about themselves. This is possible only if they are made aware of the fact that such collection, storage, use, communication etc. occurs or is likely to occur in a particular setting. The *Principle of Openness* therefore entails that patients who enter a setting where data about them are collected or communicated, etc. should be alerted to this fact. The reason for this is that the potential subjects of data-gathering might not wish to have health care data gathered about themselves and who, if they knew that this would take place, would adjust their behaviour to avoid such data being gathered. For example, such individuals might then avoid using the health care facilities or eschew consulting health care providers who engage in data gathering. While this might—and indeed probably would—seriously reduce the possibility of such persons receiving appropriate and necessary health care and potentially jeopardize their health status, they do have that right. This right, although it may be imprudently exercised, is grounded in the fundamental ethical *Principle of Autonomy*, and is reflected in the World Medical Association's Code of Ethics.[xxix]

2. ***HIPs have a duty to ensure that appropriate procedures are in place so that:***
   a. electronic health records are established or communicated only with the voluntary, competent and informed consent of the subjects of those records, and

   b. ***if an electronic health record is established or communicated in contravention of Clause* A.2.a*, the need to establish or communicate such a record has been demonstrated on independent ethical grounds to the subject of the record, in good time and in an appropriate fashion.***

This clause deals with the process of actually establishing, maintaining and communicating electronic health records. It deals with the procedural safeguards that are necessary to ensure that EHRs are established and communicated only in an ethically appropriate manner. The general duty that is enunciated in the first part of this clause derives from the Principle of Information Privacy and Disposition. It means that HIPs cannot simply assume that the data development, retrieval and processing systems with which they are involved in a professional capacity meet the ethical requirements of informed consent on part of the subjects about whom data are being gathered, used or communicated. Instead, HIPs have a positive duty to satisfy themselves that this is indeed the case. It therefore implies that HIPs cannot simply adopt a passive and accepting stance in this regard. Moreover, the clause also entails a positive duty to take appropriate steps that are designed to correct the situation if indeed the appropriate safeguards are not in place.

The second part of this clause is based in the Principle of Legitimate Infringement, the Principle of Accountability and the Principle of Least Intrusive Alternative. It focuses on the ethical limitations of the procedures under *Clause A.2.a*. These limitations are grounded in the fact that all persons who are embedded in a social context receive benefits from that embedding. This is especially clear in the context of health care.

More specifically, modern health care would be impossible if the members of society who benefit or expect to benefit from health care did not co-operate in its planning, development and delivery. Not only individual health care but also public health measures, the training and education of health care professionals, health research, etc. are all implicated in this regard. If relevant data were not developed and available, none of these would be possible and health care in any meaningful sense would disappear. This is true even if the health care system in question does not have an allopathic focus. Therefore, whoever benefits from or expects to benefit from a health care system, whether that be in an institutional setting or on the basis of interactions with individual health care professionals, has a duty to permit a limited infringement of their otherwise absolute right to privacy and to allow data about them and about their condition to be gathered, stored, manipulated, communicated, et.—where of course the nature and extent of such actions should be demonstrably necessary for the health care system in question to exist and function. At the same time, as follows from the Principle of the Least Intrusive Alternative, any such infringement should always be to the least degree necessary to achieve these otherwise legitimate aims. Moreover, any such infringement must always be justified to the subjects about whom the data are being gathered so that they may challenge the infringement if the affected individuals should consider it ethically appropriate to do so.

3. HIPs have a duty to ensure that the subjects of electronic health records are made aware that

a. an electronic health record has been established about them,

b. who has established the record and who continues to maintain it,

c. what is contained in the electronic health record,

d. the purpose for which it is established,

e. the individuals, institutions or agencies who have access to it or to whom it (or an identifiable part of it) may be communicated,

f. where the electronic health record is maintained,

g. the length of time it will be maintained, and

h. the ultimate nature of its disposition.

While *Clause 2* outlines the general conditions that an informatic framework involved in establishing, communication and otherwise handling EHRs should meet and the duties that arise for HIPs professionally who are associated with its establishment, functioning and maintenance, *Clause 3* deals more specifically with the actual operation of such a framework and the role that HIPs play in this connection. The various provisions mentioned in *Clause 3* are grounded in the Principle of Openness and the Principle of Accountability. However, it is important to note that adherence to *Clause 3* does not mean that on each occasion that data are gathered, communicated or otherwise used, the subject of the data must be apprised of this fact, or that HIPs have a duty to ensure that this is the case. Not only would this be impossibly onerous—and hence in contravention of the general and fundamental ethical Principle of Impossibility—it would also interpose an insuperable barrier to the timely and efficient functioning of the health care system itself and to the providing of health care. Rather, it means that HIPs have a duty to ensure that the general informatic framework that has been developed in order to meet the conditions mentioned under *Clause 2* is transparent and is specific enough to safeguard patient rights, and that it functions appropriately.

4. HIPs have a duty to ensure that the subjects of an electronic health records are aware of the origin of the data contained in the record.

This clause is grounded in the informatic Principle of Openness. It is based on the fact that data are not always gathered or communicated in the same way. Some of them are gathered or communicated through telemetry, others through interviews with third parties, still others through personal history-taking or clinical examination, etc. Since the way in which the data are gathered may affect their accuracy, validity or relevance, and since it may also reflect on the appropriateness of the process that is used to derive the data, it is ethically appropriate that the subjects of the data be aware of their origin so that they may exercise the rights that follow from the Principle of Information Privacy and Disposition, as outlined in the preceding clauses.

However, the duty that is herewith identified is not all-encompassing. Since it is a duty that falls to HIPs only insofar as they are professionally active, it extends only as far as the HIPs' domain professional action is concerned. That domain does not include the particular characteristics of the professional interactions between health care professionals and patients. It therefore does not extend to the data themselves as these may originate in HCP-patient interactions. It extends only to the structure of the electronic health record itself and its embedding. More specifically, it entails that insofar as electronic health records contain patient-relative data, the records should be structured in such a way as to make it possible for the subjects of these records to be aware how the data that are contained in them originated. In other words,

the records and the framework in which they are embedded should be meta-data transparent. In that sense, *Clause 4* should be seen as complementing *Clause 1* and *Clause 3*.

5. HIPs have a duty to ensure that the subjects of electronic health records are aware of any rights they may have with respect to:

a. access, use and storage,

b. communication and manipulation,

c. quality and correction, and

d. disposition

of their electronic health records and of the data contained in them.

Clauses 1 to *4* outline a series of rights that belong to the subjects of electronic health records and that HIPs are ethically bound to respect and safeguard. However, the subjects of electronic health records cannot exercise these informatic rights if they are unaware them. Ignorance in this regard, therefore, would have the effect of stripping the subjects of the records of their informatic rights. *Clause 5* addresses this matter. It states that HIPs have a positive duty to ensure that the subjects of electronic health records are aware of these rights.

More than mere privacy is here at stake. Quite aside from the fact that the data that are contained in EHRs may be important to their subjects from a personal perspective—the Principle of Information Privacy and Disposition is here implicated, as are the *Principle of Access* and the Principle of Openness—they may also have economic, legal and other significance for their respective subjects. Among other things, therefore, this clause not only has relevance within the context of health care delivery but assumes increasing importance in an era of biological, medical and genetic engineering. The reason that these considerations lead to a duty for HIPs is that the latter's actions are instrumental in establishing, maintaining and facilitating the functioning of the informatic frameworks within which the relevant records are contained, accessed or manipulated. Therefore HIPs, insofar as their action or lack of action contributes to the ethical functioning of the informatic framework within which the relevant records are embedded, have a fiduciary duty towards the subjects of electronic health records to ensure that the latter are aware of any rights they may have in this regard.

6. HIPs have a duty to ensure that

a. electronic health records are stored, accessed, used, manipulated or communicated only for legitimate purposes;

b. there are appropriate protocols and mechanisms in place to monitor the storage, accessing, use, manipulation or communication of electronic health records, or of the data contained in them, in accordance with section A.6.a;

c. there are appropriate protocols and mechanisms in place to act on the basis of the information under section A.6.b as and when the occasion demands;

d. the existence of these protocols and mechanisms is known to the subjects of electronic health records, and

e. there are appropriate means for subjects of electronic health records to enquire into and to engage the relevant review protocols and mechanisms.

Clauses 1 to *5* deal with the rights of subjects of EHRs and with the corresponding duties of HIPs. However, while measures for identifying and addressing flaws or infelicities in a given informatic framework is a central aspect of quality assurance, this in itself is insufficient if their scope is confined to the performance of the framework at a particular point in time, nor should they be incident and complaint dependant. Rather, the measures should be designed to be responsive to issues independently of incident reports or complaints, and should be sensitive to possible infelicities that may arise as conditions change. Therefore, to maximize the likelihood that the informatic framework in which EHRs are embedded and used functions in an ethically appropriate fashion as its various data handling systems and approaches evolve, a proactive quality assurance program should be in place.

Furthermore, the fact that an informatic framework is transparent and proactive in the sense just indicated does not mean that measures are in place to address any issues that may be identified. In particular, it does not mean that there are appropriate protocols that would allow the subjects of EHRs to engage suitable mechanisms to deal with what they perceive to be unacceptable situations.

Clause 6 addresses both of these issues. It states that there should be appropriate and proactive protocols to monitor, on an ongoing basis, the way that the establishment, storage, accessing, use, manipulation or communication, etc. of EHRs and of the data contained in them occurs, and that these protocols should be sensitive to actual and potential changes in the make-up and functioning of the overall informatic framework. It also states that not merely should their existence be transparent, but that there should be appropriate means for the subjects of the EHRs to engage the procedures that would address any shortcomings that might be identified in this regard.

The reason all of this is a matter of ethical obligation for HIPs is the same as what underlies *Clause 6*: HIPs are instrumental for the existence and functioning of the information handling framework within which the establishment, maintenance, communication, use etc. of electronic patient records occurs. Consequently, they have a fiduciary duty towards the subjects of the electronic health records.[xxx] For that reason, also, HIPs have a duty to make sure not only that the existence of these protocols, and the means of engaging them, are known but that there are such means in the first place. As will be clarified further in the discussion of Claus E of this Code, a corresponding obligation extends towards the institutions or other parties by whom the HIPs are employed in a professional capacity because, when HIPs work in such a context, they function as their employer's agents. The thrust of *Clause* 6, therefore, is to ensure that the rights and duties that have been outlined in the preceding clauses are in fact operationalized.

7. HIPs have a duty to treat the duly empowered representatives of the subjects of electronic health records as though they had the same rights concerning the electronic health records as the subjects of the records themselves, and that the duly empowered representatives (and, if appropriate, the subjects of the records themselves) are aware of this fact.

The importance of this clause cannot be overestimated. To see why this is the case, it may be useful to briefly consider the notion of patient decision making and to relate it to the role that substitute decision making plays in this regard.

That is to say, *Clauses 1* to *6* and their accompanying explanations and discussions have essentially assumed that the subjects of EHRs are competent persons who can exercise their informatic rights on their own behalf. The reason the considerations that were raised in these clauses are important is that, as the World Medical Association (WMA) *Code of Ethics* notes, a competent patient has the right to accept or refuse treatment.[xxxi] However, one cannot reasonably make a decision to accept or reject treatment unless one has adequate and relevant information about what is involved. This extends beyond being informed about the nature of the interventions themselves but also encompasses knowledge about one's own condition since, absent such knowledge, the consequences of accepting or rejection a particular treatment will be unclear. In the context of modern health care, much of the relevant information about oneself is contained in one's EHR. It follows that if the stipulation of the WMA is to be honoured, patients must have access to their EHRs since otherwise their decision making will be uninformed and essentially blind. Consequently patients' access to their EHRs and to the data contained in them is central to their ability to make informed health decisions.

The relevance of this for HIPs lies in the fact that HIPs are the individuals who maintain the informatic systems in which EHRs are generated, stored, manipulated, accessed, communicated, etc. In other words, as has been emphasized repeatedly, HIPs are instrumentally involved in the establishment, use and operation of EHRs and the informatic systems in which they are embedded. As was pointed out above[xxxii] and indeed is clear from the meaning of the term itself,[xxxiii] individuals who are instrumentally involved in the violation of a right—and as the WMA *Code* makes clear, the right to make informed health care decisions is such a right—are complicit in a violation of that right. Consequently, HIPs have a duty to ensure that patients are aware of their right to access their EHRs and have the means to do so.

Clauses 1 to *6* have outlined the implications of this for HIPs in relation to competent patients. However, nowhere were the terms 'competence' and 'decision making capacity' clearly defined. It was tacitly assumed that their meaning was clear and the same in all jurisdictions. That assumption, however, is mistaken—a fact that assumes crucial importance when health care crosses judicial boundaries, as it does in some forms of eHealth, telemedicine and the like. Thus, in some jurisdictions the deciding criterion for competence or decision making capacity is not cognitive or psychological in nature but centres in the age of the individual.[xxxiv] In these jurisdictions persons who are below a certain age will be considered to lack competence and decision making capacity in matters of health care, and cannot freely make health care decisions on their own behalf.[xxxv] Consequently, in such jurisdictions health care decision making authority resides in their duly empowered substitute decision makers, and it is the latter who not only have the

right to access the individual's EHR but also have the right to decide whether that individual may have access to the record or to a part of it. In other jurisdictions age by itself is only treated as a *prima facie* indicator and may be ignored if, on assessment, the individual is shown to have cognitive, emotional and volitional maturity and independence.[xxxvi,xxxvii]

The issue of who counts as a competent patient is therefore important when deciding whether a given individual has a right of access to her or his EHR. Since HIPs play a central role in managing the access structures for EHRs, it is important that HIPs ensure that such access structures are in keeping with the legal requirements of a given jurisdiction. This may become difficult for HIPs if they are involved in methods of delivering health care that has an interjurisdictional footprint, such as some forms of eHealth or telemedicine. Nevertheless, any difficulty notwithstanding, the ethical duty to take appropriate steps in this regard remains.

However, all of this merely sets the stage for *Clause 7.* It is precisely when the informatic framework is responsive to these considerations and distinguishes between competent and incompetent persons that the issue of representatives or duly empowered substitute decision makers and their right of access to EHRs arises. Individuals who previously were competent may become unconscious or otherwise lose decision making capacity—for instance, when they come to suffer from dementia or for a variety of other reasons are no longer capable of making reasoned decision. However, ethically as well as legally, incompetent individuals are just as much persons as those who are competent, their lack of competence and decision making capacity notwithstanding. The deciding criterion is whether they are living persons.[xxxviii] The Principle of Equality and Justice, therefore, entails that they do not lose their right to accept or reject treatment. That would amount to discrimination on the basis of disability and would violate the Principle in question. Rather, it entails that some means must be found for exercising that right on their behalf. A duly empowered substitute decision maker assumes that role[xxxix]

It is tempting to assume that in such situations, health care decision making authority automatically falls to the attending physician or to another appropriate health care professional such as an ambulance attendant, first responder or similarly placed individual. While traditionally that was the standard assumption, and while it is still accepted as a matter of law in some jurisdictions, modern medical and clinical ethics have generally rejected this paternalistic perspective. Instead, it has increasingly come to be accepted that except in those emergency situations where the *Doctrine of Emergency* applies, the duly empowered proxy or substitute decision-maker for an incompetent person is not the physician or other health care professional but an otherwise duly empowered substitute decision maker, who then takes over the decision making role in such a situation.

As to the *Doctrine of Emergency*, the evolving understanding of this notion is that more than merely the necessity of dealing with the relevant situation in a timely and appropriate manner is involved. Instead, it suggests that the attending physician or other relevant health care professional assumes decision making authority in matters of health care if and only if the following conditions are met: *first*, health care is required to save the individual's life or to prevent serious harm; *second*, time is of the essence; *third*, there is no relevant and reasonably available advance health care directive that has previously been executed by the affected person when competent and that applies to the situation in question; and *finally*, it is

impossible or impractical to obtain the consent of an otherwise duly empowered substitute decision maker to deal with the situation.

It is also important to note that who constitutes a duly empowered proxy or substitute decision makers may vary from jurisdiction to jurisdiction and even from context to context within a given jurisdiction. However, HIPs have a duty to ensure, to the best of their ability, that the rules that apply in the context in which they work reflect the ethical and legal understanding that is standard in the relevant jurisdiction. Thus, as instrumental agents in the functioning of the informatic framework in which they work, HIPs should take appropriate steps to ensure that the informatic framework in which EHRs are embedded is sensitive to the fact that substitute decision making is not necessarily all-encompassing in scope. For instance, having substitute decision making authority in matters of finance may not entail having substitute decision making power in matters of health care. Whether they are combined again varies from jurisdiction to jurisdiction, and in most cases a separate determination to this effect has to be made either by the incompetent person when competent or, absent such a determination, by the courts. As was said, HIPs have a duty to be aware what rules apply in the case of substitute decision making so that the informatic framework in which the EHRs are embedded and in which the HIPs work includes appropriate provisions to ensure that only the duly empowered substitute decision makers will have access to patients' records.

It may be useful to note that in most jurisdictions, a court-appointed substitute decision maker takes priority over everyone else, and absent a court-appointed substitute decision maker, the next in line is generally whoever happens to have been appointed by the incompetent person when the individual was competent. This patient-appointed individual takes priority over anyone else even if he or she is not related to the incompetent person in any standard meaning of that term. This is ethically grounded in the Principle of Autonomy. When neither of these is the case, the order of priority is usually, in descending order of priority, as follows: spouse, children, parents, siblings, and others related to the individual in question. This, however, may depend on the socio-cultural determinants of the society in question. Thus, in some jurisdiction a familial model of decision-making would overrule what would otherwise be an individual and autonomy-focused model.[xl]

Ethically as well as legally, duly empowered substitute decision makers have both the right and the duty to make health care decisions on behalf of the incompetent persons. However—and this takes the discussion back to the wording of *Clause 7*—such decision making would be blind unless there was access to the information that is contained in the patients' EHRs. Consequently duly empowered substitute decision makers have the same right of access to the incompetent patients' EHRs as the patients themselves if they were competent and had decision making capacity. Therefore HIPs have a duty to ensure, to the best of their ability, that there are appropriate protocols in place that would allow identification of such a substitute decision maker, and that procedurally there are no informatic barriers that would prevent such an individual from accessing the relevant records. This may become difficult in the context of eHealth when the delivery of informatic services crosses jurisdictional boundaries and different rules apply. However, the Principle of Integrity demands that HIPs make a creditable effort in this regard.

8. HIPs have a duty to ensure that all electronic health records are treated in a just, fair and equitable fashion.

This clause follows from the Principle of Equality and Justice. The Principle states that all persons are equal insofar as they are persons, and that therefore they have the same fundamental rights. Any difference in their treatment—and, as will become clear in a moment, this includes how their EHRs are treated—must be defensible in terms of an ethically relevant difference between the individuals themselves.

This last point is worth emphasizing. The Principle of Equality and Justice does not entail that all persons should be treated in exactly the same way. Ethically relevant differences between persons require adjustment in how they are treated. To illustrate the point, some people are physically so severely disabled that they cannot walk but instead have to move around in wheelchairs. If equality and justice were equivalent to sameness, a society could say that it did not have to construct wheelchair-accessible entrances to public buildings or to make other relevant accommodations for such persons because even though failing to do so would make it difficult or even impossible for wheel-chair bound individuals to access certain buildings, they would not be discriminated against and treated unfairly because they were being treated exactly the same way as everyone else. However, as should be clear on the slightest reflection, this very sameness of treatment would be discriminatory in its effects. It would prevent individuals in wheelchairs from being able to take advantage of the opportunities that are open in that society to everyone else who can climb stairs. Therefore the society's failure to make due accommodations for the wheelchair-bound persons' disabilities would violate the Principle.

Or, take another example, all persons have the right to the security of their person. However, persons in high public office—for example, Ministers of the government or people in important and sensitive public positions—are potentially exposed to special dangers precisely because of their position or the public office that they hold. For this reason, such individuals are entitled to special protection at public expense, whereas individuals who are not in such public positions are not so entitled. In other words, the fact that the individuals are in a high position of public service constitutes an ethically relevant difference that merits special consideration.

With due alteration of detail, similar considerations apply in the case of EHRs. While all persons have the right to expect that HIPs will exercise due diligence in the treatment of their EHRs and that the latter will be handled in a fair, just and equitable fashion, and while they have the right to expect that HIPs will be equally punctilious in the care they take with the procedures, protocols, devices etc. that they use to construct, store, access, manipulate, communicate and in general deal with their records, this does not entail that all EHRs should always be treated in the same way. That would be to confuse equality and justice with sameness. As was pointed out, equality and justice does not reduce to not sameness of treatment. It means taking ethically relevant differences into account. In this case it means that the treatment of the EHRs of people who are in these special sorts of positions will have to be adjusted to compensate for any issues that might arise because of the special positions that their subjects occupy. Consequently HIPs have a duty to make sure that the informatic frameworks in which the EHRs of such individuals are to be found, and the relevant protocols that are associated with establishing and handling them, have provisions for making appropriate adjustments in such cases. Rather than violating equality and justice, it is what is entailed by the Principle of Equality and Justice itself.

To sum up, the Principle of Integrity entails that HIPs have a duty to do their best for each and every persons. However, the Principle of Equality and Justice entails that if there is an ethically relevant difference between individuals, HIPs have a duty to take appropriate steps to ensure, to the best of their ability and within the resources that are available, that the information handling framework within which they work has some effective way of identifying or flagging EHRs that require special consideration because of the ethically relevant differences of the subjects of these records, and that the EHRs that have been thus identified or flagged do in fact receive such special care and consideration. This may be difficult to achieve when eHealth crosses jurisdictional boundaries, such as in some types of eHealth and telemedicine, or when informatic services are outsourced and are provided in a jurisdiction whose laws are different from those of the jurisdiction in which the subject of the EHR resides or the relevant health or medical services are provided. However, the Principle of Integrity entails that HIPs who work in such an environment have a duty to do their best to develop and bring about the relevant modifications in the measures that would otherwise obtain.

9. HIPs have a duty to ensure that appropriate measures are in place that may reasonably be expected to safeguard the

a. security,

b. integrity,

c. material quality,

d. usability, and

e. accessibility

of electronic health records.

.

Clauses 1 to *8* have dealt with the informatic rights that belong to the subjects of electronic health records and the corresponding duties that HIPs have in this regard, and they address the implications for the fundamental ethical features of the informatic framework in with HIPs work and in which EHRs are embedded. *Clause 9* focuses on the ethical duties that that HIPs have to maximize the probability[xli] that appropriate measures are in place to operationalize these rights. This follows from the informatic Principles of Information Privacy and Disposition and Security, together with *Clause 7* of the *Code* as well as from the general ethical principles of Integrity, Beneficence and Non-Malfeasance.

It is important, however, to note what *Clause 9* does not say: It does not say that HIPs have a duty to guarantee that the integrity, security, material quality, etc. of EHRs are in fact guaranteed no matter what, and that therefore HIPs will have failed in their professional duty if an untoward informatic event does occur. The reason *Clause 9* does not say this is that, as the Principle of Impossibility states, one cannot have a duty to do the impossible.[xlii] The fact is that it would be impossible to fulfil such an absolute duty. Even when HIPs do their best to prevent untoward occurrences from happening, it is still possible that

someone will compromise the security of the informatic system and access, modify or otherwise interfere with the patient records. Hackers are a fact of life, and while HIPs have a duty to make untoward and unauthorized actions as difficult and as unlikely as possible, there is no way to guarantee that this cannot occur. There is also no way that HIPs can prevent unforeseen—and unforeseeable—accidents from compromising the accessibility, quality or usability of EHRs. Accidents do occur—as do disasters. The best that HIPs can do is plan for such eventualities, do their best in planning, and to try and minimize any untoward effects when such events occur. That is all that the Principle of Integrity can demand. If HIPs have done the best that is possible under the existing circumstances and the unforeseen and unforeseeable does occur, the Principle of Impossibility will exonerate them. Of course achieving this assumes that HIPs will have done their best to put into place an appropriate risk assessment and reduction strategy in the first place—but that is entailed by the Principle of Integrity, and goes almost without saying.

10. HIPs have a duty to ensure, insofar as this lies within their power, that an electronic health record or the data contained in it are used only:

a. for the stated purposes for which the data were collected; or

b. for purposes that are otherwise ethically defensible.

This clause follows from the Principle of Information Privacy and Disposition, the Principle of Legitimate Infringement and the Principle of the Least Intrusive Alternative. Specifically, the Principle of Information Privacy and Disposition entails that all other things being equal and in the absence of otherwise supervening and legitimate interests, patients have a right to privacy and to control access to, communication of and the use of identifiable data about themselves. Exceptions to this have to be justifiable in terms of the treatment that patients receive or expect to receive, or the equal and competing rights of others—for instance when epidemiological or similar issues are at stake.

Generally, this is not a problem because in a properly maintained health information framework patients will have been informed about these matters, will have given informed consent to the collection and use of data about themselves.[xliii] As was indicated in the discussion of *Clause 3*, that understanding derives from the statement-of-purpose that should always precede the collection and communication of patient data. Therefore, any use of the data that goes beyond the limits of this statement-of-purpose constitutes a *prima facie* violation of the Principle of Information Privacy and Disposition. The fact that these data may be extremely useful for other purposes, and the fact that it may be quite efficient simply to use the data that have thus been developed, does not alter the fact that such usage would generally be unethical. Convenience and ease of operation do not trump ethics.

At the same time— and this addresses the question of what is contained under the locutions '*prima facie*' and 'generally—the planning and delivery of health care is a social enterprise that is data-dependent. Consequently, there may be situations where it may be appropriate to use patient data that have been gathered for one purpose in a manner that was not mentioned in the statement-of-purpose for the initial gathering of the data. An example of such extraneous use might be bona fide research, or epidemiological and planning purposes that go to the common welfare. Another purpose may be to engage in quality

assurance, which is mandated for administrative and other purposes and without which the whole health framework could not satisfy the Principle of Integrity. However, it bears repeating that any such extraneous use must always be justifiable on ethical grounds, and that it must always be in keeping with the Principle of Legitimate Infringement and the Principle of the Least Intrusive Alternative. This means that if the otherwise legitimate purpose of accessing and using such data can be achieved by other means or anonymizing or de-identifying the relevant data, then there lies an obligation to do so.

HIPs are in a good position to be aware of such extraneous data use. Hence their fiduciary duty towards the subjects of electronic health records entails that they have an obligation not to participate in extraneous data use that is not ethically defensible, and to make certain that if there are ethically defensible reasons for using them in this way that except for emergency contexts where the welfare of the subjects of the records is at stake and identity is crucial, the data are as de-identified and anonymized as possible, keeping in mind that techniques of re-identification are constantly advancing.[xliv] Further, HIPs have a fiduciary duty to do their best to develop and implement data handling measures and protocols that will promote appropriate and ethically defensible data handling not merely by their informatic colleagues but also by anyone who has access to patient-relative data.

Of course, HIPs cannot be expected to guarantee complete success in this regard but only to do the best they can under the circumstances. This duty extends both to the technical devices and means that are deployed as well as to the protocols that govern their application and usage. At the same time, HIPs also have a duty to do the best they can to ensure that, all other things being equal, the subjects of the data are made aware of such extraneous use—preferably before any such ethically defensible extraneous use occurs, and preferably on the basis of an informed consent to this additional usage.

11. HIPs who are professionally involved in the establishment, maintenance or conduct of eHealth have an obligation

a. to take all reasonable steps to ensure that the rules, regulations and procedural guidelines that govern the informatic practices and services of the eHealth providers with whom they are professionally associated are consistent with the informatic rights of the subjects of electronic health records in

i. the eHealth providers' jurisdiction of incorporation,

ii. the jurisdiction where the records are stored, accessed, used, linked, manipulated or communicated by the eHealth providers, and

iii. the jurisdiction in which the subjects of the records receive the services that are delivered by the eHealth providers;

b. to take all reasonable steps to ensure that the eHealth providers with whom they are professionally associated have effective measures in place to ensure that the individuals who are served by the eHealth providers are aware of their informatic rights, and have effective means in place for addressing any disputes or matters that may arise in this regard;

c. to take all reasonable steps to ensure that the eHealth providers with whom they are professionally associated have effective measures in place to review and, if necessary, to appropriately amend the measures indicated under 11(a)-11(b) on a regular basis in order to ensure that they are consistent with evolving informatic standards and laws in the eHealth providers' domains of operation; and

d. to engage in a professional capacity only with those eHealth providers whose operative frameworks meet the standard enunciated in 11(a)-11(c).

Modern health care takes various forms of delivery. In its simplest form, it consists in the direct and unmediated interaction between the health care professional and the patient both of whom are situated in the same location or setting. In a more complex form, it involves the electronically mediated interaction between the patient and the HCP who are not be situated in the same geographic location but in the same jurisdiction, and where the diagnostic and other patient-relative data are developed and transmitted from the patient's location to the HCPs location. A still more complex form involves not merely a geographic difference between HCP and patient and the use of electronically developed and transmitted diagnostic patient data but also the provision of treatment itself at a distance, including telemonitoring of patient functions. Other more complicated forms of delivering health care at a distance are possible—or instance, telesurgery—and the types of services that are available are constantly being expanded. All of these methods of delivering health care depend on HIPs, but the ethical issues they present are essentially of the same type.

When patients and HCPs are situated in geographically distinct locations and these locations are in different jurisdictions, eHealth presents a whole new series of ethical issues for HIPs The distinct jurisdictions may be culturally distinct and differ in their views on the nature health care, privacy, the health care professional-patient relationship[xlv] and related matters. Consequently, patients and HCPs may have different views on what informatic rights—if any—patients have regarding EHRs and the whole process of data gathering, storing, accessing, communicating, linking and manipulating. The situation becomes still more complicated when the individuals who are located in these geographically distinct locations have not only culturally distinct view on these matters but the legal provisions that govern the informatic rights of the subjects of electronic health records differ between the jurisdictions.

Under these sorts of circumstances HIPs, as instrumental facilitators of the whole eHealth fabric that connects HCPs and patients, have an obligation to do their best to ensure that the rules, regulations and procedural guidelines that govern the informatic corporate structure of the eHealth providers with whom they are professionally associated and under whose auspices the relevant services are provided do not infringe on and are consistent with the informatic rights of the subjects of electronic health records. Moreover, since eHealth providers may be incorporated in one jurisdiction, provide their patient-relative services in a second jurisdiction and base the informatic aspects of their health care provision in a third jurisdiction, this means that HIPs then have the further duty to ensure that the informatic rights of the subjects of the EHRs are not overruled by the legal provisions that exist in the jurisdiction where the records are stored, accessed, used, linked, manipulated or communicated by the eHealth providers.

The ethical Principles that ground these obligations are Equality and Justice and Integrity. As is clearly enunciated in Article 1 of the *Universal Declaration of Human Rights*, all persons are equal as persons, and legal provisions that deny or violate this equality are ethically indefensible. As the *Declaration* further specifies in Article 12, all persons have the right to privacy. Therefore the fact that the administrative web of eHealth spans distinct jurisdiction cannot, ethically, be a reason for narrowing or curtailing the informatic rights that the subjects of EHRs otherwise have; and correspondingly, HIPs are ethically bound to do their best to ensure that these rights are recognized by the eHealth providers with whom they are professionally affiliated.

Further, HIPs have a duty to do their best to ensure that the subjects of the EHRs are aware of any difference between their informatic rights in their own jurisdiction and those of the eHealth provider's. This is merely an eHealth version of the duties that were indicated under **A.5** above.

Moreover, HIPs have a duty do their best to ensure that the eHealth providers with whom they are professionally associated have effective measures in place for addressing any disputes or matters that may arise in this regard. Failure to do so constitutes a breach of the fiduciary duty owed by the HIPs to the subjects of the records. For the same reason, based on the Principle of Integrity, they have a duty to take all reasonable steps to ensure that the eHealth providers with whom they are professionally associated have effective measures in place to review on a regular basis and, if necessary, to appropriately amend the informatically relevant measures they use in providing eHealth so that these are consistent with evolving informatic standards and laws in the eHealth providers' as well as the subjects' jurisdiction.

Whether these duties can be met successfully, of course, depends to some degree on the institutional or organisational framework of the eHealth provider in which the HIPs work or to which they provide their services. However, as is indicated in clause **11.d**, when that framework does not permit the HIPs to fulfil their duties in an ethically appropriate fashion, they should not enter into a contractual relationship with the institution or organisation in the first place or, if already employed, terminate their association.

12. HIPs have a duty to ensure that the subjects of electronic health records are made aware in good time and in an appropriate fashion of possible breaches of the preceding duties and the reason for such breaches.

HIPs have a duty to do the best they can to safeguard the security of EHRs. The reasons for this have already been outlined in the discussion of the preceding clauses of this *Code*; and as has also been pointed out, this goes to the integrity of the professional. However, sometimes it is impossible to provide the best possible service simply because the relevant resources are not available or because, despite their best efforts, circumstances conspire to diminish the quality of their services. Moreover, HIPs may be aware of developments or circumstances that might compromise their ability to provide as secure, as efficient and qualitatively as good a service as otherwise might be expected. If HIPs have reasonable grounds to believe that this may be the case, their fiduciary obligation to the subjects of EHRs entails that the HIPs should make certain that the subjects of these records are aware of these limitations. This duty follows not only

from the general ethical Principles of Beneficence and Integrity, but also from the informatic Principle of Accountability. It may be worth mentioning in this connection that a corresponding duty to the same effect exists towards the institution, organisation or the employers with whom the HIP stands in a contractual relationship.[xlvi] Finally, it may also be appropriate for HIPs to consider whether it is appropriate to take steps to alert the subjects of EHRs of the development of quantum computing and the implications that this, when realized in available technology, will have in limiting the privacy of their records and of the confidentiality of the latter's communication.

B. Duties towards Health Care Professionals

Modern health care professionals (HCPs) depend on EHRs and on the electronically mediated communication and informatic services that are provided or supported by HIPs. This dependence may be contractually based either directly, as in the case of individual physicians who provide patient care in their own clinics, or indirectly or in a derivative manner, as is the case when both HCPs and HIPs are part of an institution such as a hospital and it is the latter that holds the contract for the HIPs.[xlvii]

That is to say, providing modern health care, whether at the hands-on level or at the design or planning stage, is an information-intensive enterprise, and the reason that health information is gathered, stored, communicated and manipulated, etc. is not for its own sake: It is to assist in the delivery of health care. In fact, without electronic data gathering, manipulating, storing and communication, etc. technology HCPs would be hard pressed to fulfil their mandate. The implementation and use of this technology relies on HIPs. At the same time, while HIPs play an important and even enabling role, they are supportive and not the primary players in the actual delivery of health care. The main role belongs to the HCPs who actually deliver the care. This primary role of HCPs in providing care, coupled with their dependence on the technological support that HIPs provide, creates a series of obligations on part of HIPs towards HCPs. These duties towards HCPs may be expressed as follows:

1. **HIPs have a duty**

    a. to assist duly empowered HCPs who are engaged in patient care or planning in having appropriate, timely and secure access to relevant electronic health records (or parts thereof), and to ensure the usability, integrity, and highest possible technical quality of these records; and

    b. to provide those informatic services on which the HCPs rely to carry out their mandate.

The duties that are enunciated in this clause derive from the general ethical Principle of Integrity. In practice, this not only means that HIPs should provide efficient service but also that they should be

proactive in identifying and, if appropriate, developing methods, techniques and technologies that might assist HCPs in carrying out their mandate.

It may be appropriate at this juncture to point out that the phrase "HCPs who are engaged in patient care or planning" refers not only to physicians but extends to any professional who is engaged in the planning and delivery of health care. Thus, pathologists are included, as are nurses, policy analysts, quality-assurance managers and other related professionals. While their special technical expertise may not be specifically medical in nature in a hands-on sense, it is integral to the functioning of the health care system and does extend to patient care or planning. Hence the informatic needs of such individuals are included under this clause.

Further, and by extension, the duties that fall under this rubric also extend towards duly qualified and authorized researchers[xlviii] since the latter, through their work and findings, expand the options that are available to hands-on health care professionals as well as health care administrators and planners. In other words, their work assists in evaluating and improving patient care and the planning of hands-on health care delivery.

Included under these duties is the duty t be aware of and to replace or update legacy systems[xlix] as and when appropriate.[l] When such replacement or updating is appropriate but does not occur—and there may be financial or other reasons beyond the HIPs' control why it does not occur—it is obligatory on HIPs to take appropriate steps to apprise HCPs of the limitations (and possible dangers)[li] that might exist because of this lack of replacement or updating. At the same time, if the legacy systems are replaced or updated, HIPs have a duty to acquaint HCPs with any changes that they should make in their behaviour or in the protocols they use as a result of the replacement or update. Correspondingly, if legacy systems are not updated or replaced, HIPs have an obligation to make HCPs aware of any changes that they should make in their informatic behaviour and in the protocols they use as and when the informatic environment changes. This is especially important in eHealth, telemedicine, mHealth and related methods of delivering health care that has contact beyond the bounds of the immediate informatic system in which the HCPs directly practice.

2. HIPs should keep HCPs informed of the status of the informatic services on which the HCPs rely, and immediately advise them of any problems or difficulties that might be associated or that could reasonably be expected to arise in connection with these informatic services.

This clause derives from the dependence relationship between HCPs and HIPs. It is grounded in the Principle of Integrity.

That is to say, since HCPs rely on health data and on electronic communication and instrumentation in its various forms to carry out their mandate, it is important for HCPs to be aware of anything that might interfere with the availability or usability of these services so that they can take appropriate steps to

minimize any adverse effects that might result from the fact that the services may be unavailable, or from any technical problems that might arise.

It should be noted that this clause refers not only to the informatic services that presently exist within the specific institution or setting in which the health care is provided but also to the informatic services that connect different institutions or settings with each other, whether these institutions or settings are in a particular location or in a distanced setting. Consequently this duty assumes special importance in situations that involve cloud storage of patient data, or when eHealth, telemedicine, mHealth etc. are involved.

This clause also recognizes a proactive duty on the part of HIPs to constantly monitor the effectiveness and reliability of the informatic services that are provided in the setting in which they are professionally active and on which the HCPs rely, and to assist HCPs in planning ways of dealing with any difficulties that are reasonably foreseeable.

3. HIPs have an obligation to take all reasonable steps to ensure that

a. HCPs who are engaged in eHealth and who depend on the HIPs' informatic services are aware of any differences in informatic rights or standards that might affect the HCPs' ability to carry out their mandate in the relevant interjurisdictional settings;

b. HCPs who are engaged in eHealth and who depend on the HIPs' informatic services are aware of any differences in the availability of informatic devices, protocols, tools etc. 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; and

c. are aware of any difference in qualitative standards of the informatic devices, protocols, tools etc. 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.

The rules, standards, laws and regulations that determine what rights HCPs have with regard to health records in general and EHRs in particular are not globally standard Thus, whether HCPs have a right of access to family records when dealing with patients, how long patient records must be kept, what tools HCPs may use in communicating patient information, how and to whom such information may be communicated, etc. is not universally the same but varies from jurisdiction to jurisdiction. The relevant standards may not even be the same within a given national jurisdiction—for instance, if health care, privacy and related issues are a matter of provincial or state jurisdiction and not regulated uniformly at the national level. Since modern HCPs rely on informatic services for carrying out their mandate, such differences may affect how the HCPs can fulfil their fiduciary obligations towards their patients. This becomes particularly important for HCPs engaged in eHealth.

This imposes an ethical obligation on HIPs who provide informatic services for HCPs, whether this be directly because of a contractual relationship between the HIP and the HCP or because both the HCP and the HIP are situated within the same eHealth organisation, to take appropriate steps to ensure that the HCPs are aware of any differences in these informatic rights so that they may adjust their profession activities accordingly.

Likewise, HCPs who are involved in eHealth may assume that the types of informatic devices, tools etc. that are available in their own location are also available in the location where they actually deliver their services to their patients. They may also assume that the informatic protocols within this overall eHealth framework are consistent and therefore require no adjustment in behaviour or action on their part. While that is a reasonable assumption, there may be occasions when this is not the case. HIPs therefore have a duty to ascertain whether that assumption is in fact correct and to make the HCPs aware of any differences that might reasonably be expected to affect their ability to carry out their health care mandate.

With due alteration of detail, similar remarks apply to qualitative standards. It is reasonable for HCPs to assume that the qualities of the informatic tools and devices on which they depend in the eHealth context are consistent throughout the eHealth framework and that the informatic protocols of that framework are uniform and geared to the same qualitative standards. However, there may be occasions when this in fact is not the case. HIPs therefore have a duty to ensure that any such differences are brought to the attention of the HCPs in due time and an appropriate manner.

4. HIPs should advise the HCPs with whom they interact on a professional basis, or for whom they provide professional services, of any circumstances that might prejudice the objectivity of the advice they give or that might impair the nature or quality of the services that they perform for the HCPs.

Health Informatics is such a complex and vibrant field that HCPs, who are hard-pressed to keep up with burgeoning developments in their own professional areas, can scarcely be expected to be familiar and up-to-date with developments in the field. HCPs at the hands-on as well as the administrative level therefore have to rely on HIPs for advice, whether that be with respect to software, hardware, informatic methodologies or any other related aspect. It is therefore important that HCPs be aware of anything that might influence the objectivity of the advice that the HIPs might give them.

For example, it would be important for an HCP or administrator to know if an HIP had a financial or similar interest in a corporation that provides (or is expected to provide) an informatic service or device, since then there would exists the possibility that the HIP might have difficultly forming an objective opinion about the suitability, reliability or quality of a service or device in question. Similarly, it may well be important for the HCP to know that the HIP had written a particular program or was responsible for a particular informatic technique. While that might make it easier to make adjustments in their functioning if the need for this should arise, it might also influence the HIP's objectivity in evaluating their suitability

and even constitute a conflict of interest. In a worst-case scenario, this might have a negative impact on patient care.

Moreover, more than objectivity is at stake. The nature and quality of the services that HIPs provide for HCPs may also be affected by the resources that are available to the HIPs. If these resources do not allow the HIPs to provide the services that are requested by the HCPs or on which the HCPs normally rely—or to provide them in a qualitatively appropriate manner—this may have a significant impact on the HCPs' ability to provide patient care. Consequently HIPs have an obligation to alert the HCPs of this fact, so that the HCPs can adjust their professional activities accordingly. With due alteration of detail, similar remarks apply regarding the condition of any devices or tools that are involved and which the HIPs normally provide.

Another factor that might impair the nature or quality of the services that HIPs provide for HCPs centres not in a possible conflict of interest or in resource limitations but in the personal status of the HIPs themselves. HIPs are human beings. As such, they are subject to misadventures of a physical as well as a personal nature. Both of these may affect how well—and indeed whether—they can provide the professional support that the HCPs need or expect. HIPs therefore have an obligation to inform HCPs in good time of any such circumstances so that the HCPs can make appropriate adjustments in their professional behaviour.

It is important to note that the obligations that have just been outlined hold for HIPs even when a health care provider outsources its informatic services to a corporation that specializes in informatic services and the HIPs are employees of the informatic service provider. While it is arguable that in such cases the duties that have been outlined primarily belong to the informatic service corporation as legal persons,[lii] the HIPs function as agents of the corporation and it is through the HIPs that the informatic service corporation meet these obligations. Consequently, these duties devolve on the HIPs as agents of the corporations.

It may be interesting to note that these considerations do not apply uniquely to HIPs. They merely outline specific instances of the general duty that all professionals have their clients, or the persons with whom they interact in a professional capacity and who rely on them for professional services, to make them aware of the possibility that the advice they give may not be entirely objective, or to tell them of any circumstances that might impair the nature or quality of the services that they provide. This is entailed by the general ethical Principle of Fidelity.

5. HIPs have a general duty to foster an environment that is conducive to the maintenance of the highest possible ethical and material standards of data collection, storage, management, communication and use by HCPs within the health care setting.

There is an old saying that unless an institution has a security culture, measures that are intended to provide informatic security will not work very well. What underlies this saying is that if security is not

second nature to the people who work in the institution but is something that is delegated to a specific individual or group of individuals, the general working environment will not be security-conscious. This, in turn, means that errors and lapses in security are much more likely to occur.

The same thing is true about ethical standards of data collection, use, management, communication, etc. Unless an institution has an ethically grounded information culture, ethical information standards are much more likely either not to be observed at all (because they are simply not integral to the working environment) or it will be assumed that the HIPs will look after the matter. Of course, HIPs are eminently well placed to deal with such matters. However, HIPs cannot be expected to supervise all uses of informatic devices or services; and once a lapse has occurred, it may well be too late to do anything about it.

HIPs are in a good position to foster an ethical information environment so that HCPs can be aware of their own duties in this regard, and so that lapses in information ethics are minimized. Unless HCPs are trained in proper informatic protocols by HIPs, the HCPs will be unaware of how to behave—and may well run into ethical (and even legal) difficulties. Therefore, HIPs would be remiss in their duties towards HCPs if they did not try to foster an environment where the ethical treatment of electronic health records becomes almost second nature. With due alteration of detail, the same considerations apply to HIPs who are not employed by the actual health care providers but are employed by an informatics service provider to whom the health care service provide outsources is requirements.

Likewise, HIPs are uniquely placed to assist HCPs in using the best material standards of data collection, storage, management, communication, etc., and in the most appropriate manner. Indeed, since HCPs rely on HIPs for technical support in this regard, an HIP's neglect to assist an HCP regarding these aspects engages the Principle of Integrity and amounts to a failure of duty. It may even involve a violation of the principles of Beneficence and Non-Malfeasance. Consequently, HIPs should encourage not only an ethical information culture in general but also an information culture that takes it for granted that every HCP will seek the cooperation of an HIP to utilize the best and most appropriate informatic techniques in the best possible way. This duty is all the stronger as the World Medical Association's *Code of Ethics* stipulates that an ethical physician shall, "when medically necessary, communicate with colleagues who are involved in the care of the same patient," where "this communication should respect patient confidentiality and be confined to necessary information."[iii] In modern health care—and this is particularly true in the case of eHealth and telemedicine—such communication will not be by word-of-mouth or in written form but almost invariably involve electronic devices and methods, thereby instrumentally involving the HIP as facilitator.

6. HCPs who are directly involved in the construction of electronic health records may have an intellectual property right in certain formal features of these records. Consequently, HIPs have a duty to safeguard:

a. those formal features of the electronic health record in which the HCP has, or may reasonably be expected to have, an intellectual property interest; or

b. those formal features of the data collection, retrieval, storage or usage system in which the electronic health record is embedded

in which the HCP has, or may reasonably be expected to have, an intellectual property interest.

Logically speaking, data are possibilities of distinction that have been identified and labelled by using a classificatory schema. Not surprisingly, therefore, different classificatory schemata, when applied to the same set of possibilities of distinction, will yield different sets of data. However, in and by themselves data are meaningless. They are, so to speak, raw. They become meaningful only when they are correlated and connected with each other within a reference framework.[liv] Therefore different ways of sorting, connecting, correlating or manipulating data will have a significant impact on how the data become meaningful. This is true about health data as much as about any other kind of data. Furthermore, what data are collected is also potentially significant because it sets the overall framework within which connection, classification and correlation will ultimately occur, and thus will determine what will eventually become information. EHRs are electronically encoded sets of data that have been developed, collected and labelled under the classificatory schemata that are characteristic of health care.

The various aspects of EHRs that have just been mentioned may be referred to collectively as their formal features. While patients have a dispositionary right over the identifiable person-specific data that are contained in their EHRs,[lv] their formal features belong to the person who developed them and constitute that individual's intellectual property. On occasion—for instance when it comes to diagnostic algorithms, unique ways of structuring data and the like—this intellectual property right may have considerable market value.

Normally HCPs, when developing health records, will use standardized tools and methodologies that have been developed by someone else. In such a case, the dispositionary right over the formal features of the record belong to that other party. However, sometimes HCPs are sufficiently expert to develop their own methodologies and tools. In such a case, unless there has been an explicit agreement between the HCP and the patient, or the HCP and the institution with whom the HCP is affiliated, the formal features of these methodologies and tools are proprietary to the HCP and the HCP has an intellectual property right in them. Similar considerations also apply to formal features of the data collection, retrieval, storage or usage system in which the electronic health record is embedded. In these sorts of cases, HIPs must make certain that the dispositionary rights of the HCP are identified and protected. Failure to do so constitutes negligence and involves the Principles of Integrity, Beneficence and Non-Malfeasance.

With due alteration of detail, similar remarks apply in the case of corporate entities that hold such rights since, as was pointed out above,[lvi] these also count as persons. Nor is this merely an abstract or theoretical matter. On occasion—for instance when it comes to diagnostic algorithms, unique ways of structuring data and the like—such intellectual property rights may have considerable market value.

C. Duties towards Institutions/Employers

There lies a general presumption that as professionals, HIPs will only enter into service contracts with employers who are engaged in ethically legitimate enterprises. That being said, once HIPs have accepted employment, they stand in a contractual relationship with whoever employs them, and the contract that seals the relationship usually spells out the nature and the extent of the services that are expected.

However, no contract can stipulate all possible details of what might happen or what sorts of situations might arise. Here the duty of loyalty that all professionals owe their employers—and therefore that HIPs owe those who employ them or with whom they stand in a contractual relationship—becomes relevant. They have a right to expect that HIPs will do their best to advance their interests insofar as this does not conflict with the duties that the HIPs owe towards the subjects of the records,[lvii] other professionals,[lviii] society,[lix] or the health informatics profession.[lx]

These exceptions are important. For instance, the duty of loyalty that HIPs owe their employers does entail that they should do their best to allow their employer to operate in as efficient and as fiscally advantageous a manner as possible; however, this does not mean that this duty overrides the HIPs' duties towards the subjects of EHRs as spelled out in Section A of the Code. It may be necessary for HIPs to use informatically less-than-optimal protocols, measures, tools or techniques if the resource base does not allow for anything else and the relevant services have to be provided; but in that case all concerned parties—in this case it would be the subjects of the records, the HIPs and the employer—should be made aware of that fact in good time so that they are able to deal with or prevent any issues that might arise in this connection.

Likewise, when the legitimate interests of third parties who have a duty towards the subjects of the records—this is true of HCPs who stand in a fiduciary relationship towards the subjects—require that they carry out certain actions that draw on informatic services that involve the actions of HIPs and the HIPs must assist them in a professional capacity in order for them to be able to carry out their mandate—then the interests of the employer must take second place.

Nevertheless, these exceptions aside, employers or institutions have the right to expect that HIPs will do their utmost to safeguard their legitimate interests. This is rooted in the Principle of Integrity. The employer or institution must be able to trust that HIPs will carry out the informatic roles and deliver the informatic services for which they have been hired, and that the HIPs will do so in the best way possible under the circumstances that obtain.

Again, this last clause is important. Under the Principle of Impossibility, it would be unfair to expect HIPs to provide services for which there are inadequate resources, or to adhere to standards that cannot be adhered to given the resources that are in place. Therefore, the settings in which HIPs operate set certain material limits which the HIPs cannot transcend—and should not be expected to transcend. At the same time, if these limits are likely to act as barriers or impediments to proper professional action, then the

HIPs have a duty to apprise the employer or organisation of this fact in an appropriate manner and in good time

It would also be ethically indefensible for employers to expect HIPs to provide informatic services that contravene ethically defensible standards and to point to the obligation of loyalty as grounding such a request. This may become particularly problematic for HIPs when their employers are engaged in interjurisdictional eHealth or related undertakings, since legal provisions may vary from jurisdiction to jurisdiction. It is not a foregone conclusion that being a valid legal requirement in a particular jurisdiction establishes it as ethically valid or binding. So, for instance, legal provisions in some countries which permit privacy intrusions that violate Article 12 of the *Universal Declaration of Human Rights* may be legally valid in that particular jurisdiction but for all that would be unethical. Thus, access to EHRs for the sake of facilitating interrogation techniques—for instance, access to EHRs to facilitate the successful use of the torture under conditions like the ones that are outlined in the Landau Commission's Report[lxi]—may be legal in some countries, but providing such services would be unethical in light of the United Nations *Convention Against Torture*.[lxii] HIPs who provided services in that regard would be complicit in any violation of human rights and could not escape responsibility on the grounds that they were just following orders from their superiors

The important thing—and this is illustrated by the diagramme of the HIPs' overall ethical embedding that was sketched above[lxiii]—is that HIPs are embedded in an overall context that involves not only organizations and patients but also other professionals and society itself. The various strands in this web of ethical relations consist of rights and obligations that at times have to be balanced, and on occasion duties that are owed toward society may override the duties that owed the subject of the records, that are owed to HCPs or those that are owed to the employers. For instance, epidemiological issues may require that the duties towards the subjects of EHRs may be overridden as well as the duties towards institutions or employers. However, these duties must always be keeping with internationally acknowledged ethical standards

With this in mind, the individual clauses in Section C of this *Code* spell out the various duties towards institutions and employers in more detail.

.

1. **HIPs owe their employers or the institutions in which they work a duty of:**

    a. competence;

    b. diligence;

    c. integrity;

    d. loyalty.

As should be clear, the conditions that are enunciated in this clause are not unique to HIPs: they derive from a general duty of integrity that is owed by everyone who is employed by, or stands in a contractual relationship to, another party. Among other things, this clause entails that HIPs have a duty to:

- not misrepresent their training, skills and abilities;
- keep current and proficient in their areas of claimed expertise, and of undergoing re-training, upskilling or retraining as and when appropriate and when the occasion so demands;
- alert their employer when a task exceeds their skills, abilities or training;
- work effectively, efficiently and diligently on their employers' behalf; and
- advise their employer when the working conditions under which they are expected to perform their tasks do not allow them to carry out their professional mandate in a proficient, satisfactory and ethical manner.

It also means that HIPs have a duty to:

- alert their employer, organisation or institution with which they are professionally associated of any reasonably credible threat to the efficient and successful informatic operations of their employer, organisation or institution, whether that threat be externally or internally based; and
- unless otherwise specified as a condition of employment, to maintain confidentiality with respect to any proprietary information and any data that would normally be considered confidential, even after their affiliation with their employer, organisation or institution has been severed.

The major ethical principles that ground these various duties are those of Integrity, Beneficence and Non-Malfeasance: Integrity, because not to adhere to these conditions is for HIPs to be negligent in fulfilling their agreed-to duties to the best of their ability and acting in the best way they can; Beneficence, because not to adhere to them is for HIPs not to advance the good of their institution, organisation or employer in keeping with the latter's fundamental and ethically defensible values, which is an obligation that HIPs accept as a condition of their employment; and Non-Malfeasance, because failure to adhere to these conditions is to for HIPs to increase the probability that their employers, organisations or institutions may suffer a setback in their operations.

2. HIPs have a duty

a. to take all reasonable steps to ensure that the informatic products, services, tools or devices they recommend to the employers, corporations or institutions with whom they are associated in a professional capacity are

(i) suitable,

(ii) reliable, and

(iii) qualitatively appropriate

so as to allow the latter to meet their informatic obligations towards the patients they serve and towards the HCPs they employ;

b. to take all reasonable steps to ensure that the informatic protocols they recommend or institute are

(i) suitable,

(ii) reliable,

(iii) effective, and

(iv) qualitatively appropriate

to allow the employers, corporations or institutions with whom they are associated in a professional capacity to meet their relevant obligations;

c. to take all reasonable steps to ensure that their employers or the corporations or institutions with whom they are associated in a professional capacity are made aware in good time of any differences in the informatic obligations that may reasonably be expected to affect the latter's operation in an eHealth context or in an interjurisdictional domain of operation; and

d. to be professionally qualified and certified, and to continue to be qualified and certified in keeping with the highest current professional standards, and if the employer, corporation or institution with whom they are associated in a professional capacity provides services in an interjurisdictional context, to meet the most stringent standards in the employer's, corporation's or institution's domain of operation.

HIPs are experts in health informatics and as such have a duty, rooted in the Principle of Integrity, to do their best in their professional environment and to carry out the duties for which they are hired. Obviously, this involves carrying out their mandated technical tasks in the best possible way.[lxiv]

At the same time, it is important for HIPs to recognize that not everything is possible in every setting, and that achieving a particular outcome or meeting a certain standard is in part context dependent. Resources may be limited, just as there may be other limiting conditions—for instance, there may be a lack of staffing that would be necessary for carrying out a particular task or for meeting a certain standard, etc. These limitations put boundaries on what it is possible for HIPs to do in that particular context or on that particular occasion, just as they put limits on what HIPs can reasonably recommend to their institutions or individuals with whom they stand in a contractual relationship.

Consequently, HIPs would not be acting unethically, nor would they be neglecting their professional duty if, under such limiting circumstances, the services they provided or the measures they recommended were not optimal in an absolute sense. It would also not mean that they would be ethically remiss if they recommended different measures in different institutional settings or if the services they provided in one setting were not up to the same standards of those they provided in another setting. The important thing is that the services they provide or the measures they recommend should be consistent with the resources that are available. Of course if the available resources were insufficient or other limiting conditions

interfered with their ability to recommend or provide the relevant services, fidelity would also entail that those who could reasonably be expected to be affected by this should be made aware of that fact.

However, HIPs would be ethically remiss if the recommendations that they made or instituted in their professional capacity, whether that be with respect to informatic products, services, tools or devices or with respect to the protocols that they instituted or recommended, were not qualitatively appropriate, reliable and effective within the available resource base, and their employers could not function in the best way possible within the limits of their resources and their identified domain of operation.

At the same time, informatic quality is very much a creature of obsolescence. Consequently, HIPs have a duty not only to monitor the quality of the informatic services relative to the existing resources provided by their employer or within the institution in which they work, but to continually survey the field of informatics relative to the foreseeable future informatic needs of their institutions or employers so that the latter can make appropriate plans or undertake adjustments in their manner of operation.

Moreover, it is not only the technical and procedural resources and protocols of an employer, institution or organisation that affect the latter's ability to operate successfully. The legal aspects of the organisation's domain of operation may also have an effect on the likelihood of their successful operation. HIPs would therefore not be fulfilling their duty of loyalty and would violate the Principle of Integrity if they did not take all reasonable steps to identify and inform their employer or those with whom they stand in a contractual relation, in good time and in an appropriate manner, of any differences in the informatic rules or regulations that may reasonably be expected to affect the latter's operation in an eHealth context or in an interjurisdictional domain of operation.

In part, all of this depends on HIPs being properly qualified and certified, and on keeping abreast of any changes or new developments that may affect how well they are able to carry out the role they have accepted when they entered into a contractual relationship with an individual, institution or organisation. Consequently HIPs have a duty not only to be professionally qualified and to maintain that qualification to the highest current professional standards in the institution's, organisation's or employer's domain of operation.

It scarcely needs mentioning that HIPs would be ethically remiss if they entered into a contractual relationship with an individual, institution or organisation if, from the very outset, it was clear to the HIPs that they could not fulfil their obligations or function in a professionally optimal manner because of the limiting conditions and they did not inform their prospective employer of this fact.

3. HIPs have a duty to

a. foster an ethically sensitive security culture in the setting in which they practice their profession,

b. facilitate the planning and implementation of the best and most appropriate data security measures possible for the setting in which they work,

c. implement and maintain the highest possible qualitative and ethical standards of data collection, storage, retrieval, processing, accessing, communication, linkage and utilization in all areas of their professional endeavour.

The best way for HIPs to meet the informatic requirements of their institutions, organisations or their employers is not merely to strive for excellence in their own work but to try to foster an ethically sensitive informatic security culture in the setting in which they work, and to attempt to instil an appreciation and expectation of informatic quality not merely in themselves but also in others who work in the same setting. This will involve all aspects of the informatic life of the institution or professional setting

There is an old saying: "It's not what you have but how you use it." A particular setting may be as resource-rich as possible, if the protocols and measures for using these are not suitable and effective for the task at hand, and if the context in which they are used is not structured in a way that potentiates their ethically optimal employment, using the resource will not result in the ethically best possible outcome. In fact, the outcome may be highly undesirable. That is why, if the data security measures in the setting in which HIPs work are not materially and operationally— but above all ethically—the best possible for that setting, then this may well jeopardize the informatic soundness and the ethical status of the whole setting, technical sophistication and resource richness notwithstanding. The organizations, employers or institutions with whom HIPs stand in a contractual relationship have the right to rely on HIPs alerting them to and advising them of possible issues in this regard, and evaluating whether what is in place is informatically and ethically sound. Consequently, HIPs have a duty, grounded in the Principle of Integrity, to facilitate the planning and implementation of the ethically best and most appropriate qualitative and procedural standards for that setting.

However, the mere existence of ethical standards is insufficient to guarantee the ethical operation of the organisation, institution or setting in question. If the organisational culture is not ethically sound, it is unlikely that its operational functioning will be as ethical as it should be. This holds true no matter what the context or setting. Trivially, therefore, it also holds true of the context or setting in which HIPs practice their profession. It is therefore obligatory for HIPs to take appropriate steps to instil an ethical cultural in general, and in particular an ethically grounded security culture, in their place of employment. This extends not merely to implementing and maintaining the highest possible ethical standards of data collection, storage, retrieval, processing, accessing, communication, linkage and utilization in light of current conditions but also to facilitating the planning of future adjustments in this regard as informatic resources, opportunities and challenges change. With due alteration of detail, similar remarks apply to qualitative standards.

4. HIPs have a duty to ensure, to the best of their ability, that appropriate measures are in place to evaluate the technical, legal and ethical acceptability of the data-collection, storage,

retrieval, processing, accessing, communication, linkage and utilization of data in the settings in which they carry out their work or with which they are affiliated.

This clause builds on the preceding. It is impossible to be sure that the informatic framework or infrastructure of an organisation or institution functions ethically, legally and technically appropriately and in a way that is best suited to meet its informatic needs—in other words, that it functions in a technically, legally and ethically appropriate manner—unless some measures are in place to monitor and evaluate its operations in this regard. HIPs therefore have a duty (rooted in the Principles of Integrity, Beneficence and Non-Malfeasance) to ensure, to the best of their ability, that appropriate measures to this effect are in place, that they function properly, and that they are reviewed and adjusted as conditions change and new challenges arise.

This duty is especially important when there is a difference between ethical soundness and pragmatic success. HIPs should never lend their expertise to the development and deployment of evaluative measures that are ethically indefensible and that are not in keeping with the principles of informatic ethics, their pragmatic effectiveness notwithstanding. The Principles of Information-Privacy and Disposition, Openness, Security, Access, Legitimate Infringement, Least Intrusive Alternative and Accountability in particular deserve special attention in this regard.

It will be clear that the duty that is enunciated in this clause takes on special importance when the organisation, employer or institution with which an HIP is professionally associated operates in an eHealth environment or a related setting, and when its domain of operation spans jurisdictional boundaries. Technical and legal standards may differ from jurisdiction to jurisdiction, and the understanding of ethical standards may be subject to different interpretations in different settings. HIPs, therefore, as instrumental facilitators of eHealth, have a duty towards their organisation, institution or employer to do their best to ensure that measures are in place to evaluate the technical, legal and ethical acceptability of the data-collection, storage, retrieval, processing, accessing, communication, linkage and utilization of data that frame the operation of their organisation, institution or employer in an interjurisdictional context, and that these are appropriate in the settings in question. They also have a duty to ensure, as best as they are able, that the evaluative measures whose purpose is to ensure this are themselves ethically beyond reproach. This may present special problems in eHealth and interjurisdictional health care, and when health care and administrative services are outsourced using electronic means.

5. HIPs have a duty to alert, in good time and in a suitable manner, appropriately placed decision-makers of the status of the security, robustness and quality of the data-generating, storing, accessing, handling and communication systems, programmes, devices or procedures of the institution with which they are affiliated or of the employers for whom they provide professional services.

The best quality assurance programme in the world is useless if those who are in decision-making authority are unaware of its results. Clause ***C. 5*** is based on this fact. It stipulates that HIPs have a duty

not merely to ensure that evaluating and monitoring programmes are in place and functioning (as is stipulated in Clause ***C.4***), but that appropriately placed decision-makers are made aware of their performance.

Normally, this means that HIPs have a duty to follow established reporting procedures within their respective institutions or for their respective employers. However, there may be occasions—for instance, when following these procedures may take too long, be too involved, or for some reason be unlikely to result in appropriate action—when HIPs may have a duty to directly approach the responsible decision-maker(s) and provide them with the relevant information. This may have difficult repercussions for the HIPs; however under such circumstances HIPs ethically have no choice. Even so, HIPs would be entitled to expect the protection of their respective institutions or employers, since they would be acting out of integrity and within their ethical mandate.

At the same time, it should be noted that the duty that is outlined in **C. 5** is limited in nature. With an exception that will be noted in a moment, the HIP's duty extends only towards the organisation, institution or employer with whom the HIP is contractually affiliated; it does not extend to third parties who provide informatic products or services. The reason lies in the difference between a vendor-purchaser relationship and an employer-employee relationship. Vendors guarantee that the goods or services they offer or supply to their purchasers will be reasonably fit for the purpose that is specified and agreed to between them as a tacit condition of sale. This establishes an ethical web of rights and obligations between the two parties. HIPs are not part of that web.

More specifically, the vendor-purchaser relationship establishes an ethical web of rights and duties between the former and the latter that is independent of and distinct from the web of ethical relations that binds employer and employee. Even though the purchaser—in this case, the organisation, employer or institution with whom the HIP is affiliated—relies on the latter's advice regarding the informatic products or services that are provided by a third party, this does not establish an obligation on part of the HIP towards the third party because the HIP is not part of the vendor-purchaser framework. Therefore, alerting or otherwise informing the vendor of any shortcoming of the informatic product or service the latter supplies does not fall into the web of duties and obligations that surround the HIP as an employee. In fact, generally it is not even the duty of the purchaser—in this case the organisation, employer or institution with which the HIP is contractually affiliated—to inform the third party of any shortcomings of the product or services that it offers for sale or that the organisation has purchased. It is up to the third party itself to take appropriate steps to ensure that the products or services that it offers are "fit for the purpose."

It may of course be important—and this refers back to the exception mentioned to above—that any shortcomings that are associated with the informatic products or services that are offered or supplied by a vendor become known. In particular, this may be the case when the products or services are licenced or accredited, because then reliance on such certificates is misplaced and may affect others. In such a case, however, the duty to make such shortcomings known is not a duty that is owed to the vendor but to the licensing, certification or accreditation authority. The reason for this lies in the notions of licensing, certification and accreditation themselves. The licensing, certification or accreditation authority is a social service provider which holds itself out as acting in a trustworthy manner when its licenses, certifies or

accredits some product or service. Both the HIP and the organisation with whom the HIP is professionally affiliated rely on the validity of the license, certification or accreditation that the authority grants. However, this whole framework of licensing, certification and accreditation presupposes that the licensing, certification or accreditation authority is aware of all relevant facts when it licenses or certifies the products or accredits services in question. Therefore as beneficiaries of this socially grounded process, the reliance that the organisation as purchaser and the HIP as professional places on the relevant process imposes a duty on them, based in Beneficence and Non-Malfeasance, to inform the authority when this reliance is misplaced. It is up to the authority to take further steps.

6. HIPs should immediately inform the institutions with which they are affiliated or the employers for whom they provide a professional service of any problems or difficulties that could reasonably be expected to arise in connection with the performance of their contractually stipulated services.

This duty parallels similar duties that HIPs have towards HCPs and towards the subjects of electronic health records. That is to say, institutions and employers have the right to expect that those on whom they rely for contractually stipulated services will actually perform these services in the agreed-upon manner.

However, there may be occasions when HIPs have reasonable grounds to believe that it will be impossible for them to live up to such expectations, or to provide the relevant services either in an appropriate manner or at an appropriate level. In such a case, HIPs have an obligation to inform their employers or institutions of this fact, and to do so in good time. External, internal as well as personal problems are implicated in this context, as is the possibility of conflict of interest. This obligation is again rooted in the Principle of Integrity and holds in all cases where an organisation, employer or institution relies on the services of those whom it employs, so the health informatics context is not an exception.

The duty also it also finds an ethical basis in the Principle of Non-Malfeasance, since failure to perform the expected and contracted services, or to perform them in the appropriate manner, may interfere with an institution's ability to meet its obligations towards its clients. Therefore it may cause harm not merely to the institution itself but also to third parties. Without adequate and timely warnings, therefore, institutional administrators cannot make appropriate decisions, and their ability to provide relevant and expected services may be seriously impaired. This clearly constitutes harm to the organisation or institution, and may well result in harm to its clients. In health care, that may be catastrophic.

7. HIPs should immediately inform the institutions, employers or agencies with whom they are affiliated or for whom they provide professional services of circumstances that might prejudice the objectivity of the advice they give.

This duty is similar to the duty mentioned in **B. 4**. It is grounded in the Principles of Integrity and Non-Malfeasance. More specifically, the Principle of Integrity stipulates that whoever has an obligation, has a corresponding duty to fulfil that obligation to the best of her or his ability. By entering into a professional relationship with an institution, organisation or employer with which HIPs have entered into a contractual relationship rely on the HIPs for advice on informatic matters, be that with respect to tools, devices, protocols, policies, etc. If this advice is not objective, it may result in inappropriate decisions being made, possibly having serious negative repercussions. Consequently, the Principle of Integrity entails that HIPs have an obligation to disclose possible areas of conflict of interest that might prejudice the objectivity of the advice they give. It also means that HIPs have a duty to make those who rely on their services aware of any physical, social, personal or psychological factors that might reasonably be expected to affect the objectivity of the advice they may tender. The same duty follows from the Principle of Non-Malfeasance; because if the institution, employer or organisation relies on the advice that is given by an HIP and this advice is not objective, and if this results in a negative outcome, then the HIP is a determining causal factor of that negative outcome.

8. Except in emergencies, HIPs should only provide services in their areas of competence, and should always be honest and forthright about their education, experience, qualification and training.

This duty finds its basis in the Principles of Integrity, Non-Malfeasance and Autonomy and Respect for Persons.

More specifically, for HIPs to misrepresent their education, experience, training or qualification is for them to lie. Not only is that unethical in itself, it may also have serious negative consequences for the individuals, organisations or institutions who employ them. That is to say, HIPs who apply for or agree to be considered for a certain position or task hold themselves out as having certain education, experience, training or qualification, and employers or prospective employers may reasonably rely on the correctness of such claims. As a consequence, misrepresentation may result in them making an inappropriate choice either by hiring such unqualified HIPs or by assigning tasks to them that can be satisfactorily performed only by someone who has these qualifications. This, in turn, may have serious negative consequences either because the HIP will be unable to fulfil the tasks in question, or because the HIP will be unable to fulfil the tasks in the expected and requisite manner.

As for HIPs only providing services in their areas of competence—i.e., not going beyond their area of education, experience, qualification and training—the reason for this is that to go beyond one's area of competence in professional matters is to venture into areas where one is unlikely to fully understand the true nature of the situation with which one is confronted or the relationships that exist in the situation in question. Further, not being trained or qualified in that area, one may lack a repertoire of appropriate actions and have to improvise—which in turn involves a significant likelihood of doing something that is inappropriate or harmful, or both. In other words, not following this injunction would violate the duty of integrity that HIPs owe those with whom they stand in a contractual relationship.

However, the world does not always unfold in a regular manner and as expected. Situations may arise where there are reasonable grounds to suppose that for HIPs not to act outside of their area of education, experience, qualification or training would result in greater harm than if they acted. Under such circumstances, the obligation that HIPs have incurred when they accept employment may well entail that they should act.[lxv] However, even in such cases HIPs should bear their limitations in mind and should not go beyond what is absolutely necessary in that situation. They should also make it clear to the relevant parties that they are acting outside of their area of competence, and should request that someone who has the requisite qualifications take over as soon as possible.

9. HIPs should only use suitable and ethically acquired or developed tools, protocols, techniques or devices in the execution of their duties.

The first part of this clause, which deals with suitability, needs no further explanation since it is firmly rooted in the Principle of Integrity and in the general duty of loyalty that HIPs owe their employers. As to the second part, which deals with the source of what is used by HIPs in the performance of their professional duties, it derives from the Principle of Equality and Justice as well as the Principle of Non-Malfeasance.

More specifically, the Principle of Equality and Justice entails that HIPs should not deprive others of the fruits of their labour. Consequently, HIPs should never use protocols, tools, techniques or devices that have not been acquired in an ethically acceptable fashion. The Principle of Non-Malfeasance is implicated because the failure to follow this injunction may have negative consequences for the originator or proprietor of the tools, protocols, techniques or devices by depriving them of what is their due. Finances and recognition may be at stake. It may also have negative implications for the institutions or employers with whom the HIPs are contractually affiliated—something that may well be the case when it involves a violation of intellectual property or patent rights.

As to the use of protocols, tools, techniques or devices that have been developed in an ethically inappropriate manner, these may be pragmatically useful but they are tainted by their origin. Therefore, arguably, to use them is to tacitly validate the conditions under which they were developed, and to encourage the ethically objectionable actions that gave rise to them. It is not surprising, therefore, that there is considerable debate over whether they can ethically be used. However the emerging consensus seems to be that they may be used if they are publicly available, their unethical origin is admitted and, above all, if great harm is avoided by using them.

10. HIPs have a duty to assist in the development and provision of appropriate informatics-oriented educational services in the institutions or agencies with whom they are professionally affiliated or for the employers for whom they work.

Lack of knowledge, training or competence limits what someone can identify as a problem or see as an opportunity in a given situation, and it also narrows the individual's domain of action. Consequently, it may lead to missed opportunities or even to mistakes being made; but in any case, it will detract from the optimal performance of the individual in question and hence interfere with the optimal functioning of the organisation or institution by which the individual is employed or otherwise detract from an employer's ability to achieve the best possible outcome in a given situation.

It would be unreasonable to expect that everyone who works in the health care setting is trained, educated and competent in all areas of health care simply because they work in the health care setting. Specialization and focus in education and training are inherently conducive to improved quality of service because they deepen the ability to diagnose and deal with issues that arise. However, this is beneficial only when the specialized skills themselves are integrated into an overall functioning framework that operates properly as a whole. This, in turn, can occur only when those who work within that framework are aware of, have some understanding of and can take advantage of what binds the relevant areas of that framework together.

What allows the various areas in the modern health care to function in an such integrated manner is informatic in nature. It involves the development, storage usage, transfer, linkage, communication and transformation of data. Therefore the more the individuals who work in that setting are acquainted with these informatic features, the better they can perform their own tasks and the more integrated and qualitatively better the framework itself will function. HIPs' are informatics specialists, and have a better understanding of the informatic aspects of the overall framework in which health care is delivered than anyone else. The Principle of Integrity entails that they have a duty to further the best interests of their employers. Therefore, unless the HIPs have entered into a task-specific relationship with their employer—which on occasion may be the case—they have a duty to assist in the development and provision of appropriate informatics-oriented educational services in the institutions or agencies with whom they are professionally affiliated or for the employers for whom they work.

.

D. Duties towards society

The duties of HIPs towards society derive from three sources:

- the fact that HIPs are embedded in a social context;
- the fact that HIPs deal with sensitive personal data; and
- the fact that HIPs are professionals.

The first source is simply the fact that HIPs do not carry out their professional activities in a vacuum. They are—as the statement has it—embedded in a social context. This means that as members of society their

behaviour is subject to the same fundamental ethical principles as those that govern all social behaviour. What these principles entail in a particular type of context may differ from profession to profession and from one kind of activity to another—how this is the case for informatics as a discipline was outlined in Part I of this Handbook—but the fundamental principles are one and the same. This latter is particularly true when the kind of activity is one that deals with ethically and socially very important and very sensitive matters.

And this introduces the second source of obligation. Not everyone is in the same position of trust, provides as sensitive and important a service, or has access to or facilitates the collection, storage, use, communication or manipulation of the same sensitive data as HIPs. Moreover, not everyone is in a position where their professional activities underwrite and make possible an entire sector of social endeavour. Modern health care would simply be impossible without the professional activities of HIPs. Therefore the social duties of HIPs are different from, say, those of grocers, architects or petroleum engineers.

Furthermore—and this is captured by the third point—the fundamental ethical principles that bind members of society bind HIPs more stringently than people who are not professionals simply because they are professionals. Society expects more from professionals because they have a greater degree of training and expertise, are in sensitive positions, and hold themselves out as being responsible individuals whom society can trust. This is all the more the case when these individuals have professional certification.

However, the duties HIPs have towards society in general may conflict with the duties that HIPs have towards identified other parties such as patients, institutions or HCPs. For example, the privacy rights of the individual patient may conflict with the information needs of society when contact-tracing or epidemiological planning is carried out. Therefore there has to be some means of resolving such conflicts of rights.

Ethically, and in general terms, a conflict resolution schema is acceptable if and only if it respects fundamental ethical principles and is consistent with the basic rationale of the service in which the conflict arises. In the present context this means that the resolution schema would have to respect the principles of informatic and fundamental ethics. Therefore the test for ethical acceptability is twofold:

- Is the infringement necessary to carry out a duty towards the patient?
- Is the infringement necessary to fulfil any otherwise over-riding duty towards others, e.g., to prevent harm to third parties?

If the answer to either of these is ‘Yes’, then it will be ethically acceptable to infringe on the rights of the subjects of the electronic records for this reason and on this occasion. However, this should always be in keeping with the Principle of the Least Intrusive Alternative. This may even be stipulated in law, as for instance when there is a concern for the safety or health of other specific persons or groups of persons.

On this basis, the following rules govern the conduct of HIPs:

1. HIPs have a duty to facilitate the appropriate

a. collection,

b. storage,

c. communication,

d. use,

e. linkage and

f. manipulation

of health care data that are legitimately used in research or that are necessary for the planning and providing of health care services on a social scale.

At first glance, this clause seems to contradict the Principle of Information Privacy and Disposition as well as the ethical guidelines for data protection and privacy as promulgate by the European Union[lxvi] and similar national or international organizations. However, the clause it is justified both ethically and legally by the Principle of Impossibility,[lxvii] which latter becomes the Principle of Legitimate Infringement in the informatic context. The reason is that without access to the relevant patient data, society cannot plan for or provide health care services. Among other things, planning health care services requires data about the incidence, prevalence and distribution of health conditions. Without such data, budgets cannot be developed nor can delivery modalities be planned in more than an ad hoc fashion.

As to research, not all health related research is primary research that originates its own data. In fact, a large proportion of health related research draws on data that have been previously developed in other contexts. Without access to such data, health research would be severely hampered and improvement in health care would be severely hampered. Moreover, checking the validity of conclusions that have been derived on the basis of primary research serves the extremely useful purpose of maximizing the probability that these data have been interpreted correctly. That is why some authorities have embarked on a process of legitimating open access to publicly funded health related research;[lxviii] and in some countries researchers whose projects have been approved by a duly constituted ethics committee have the right of access to such data as long as confidentiality is maintained. HIPs who are involved in such actions would not be acting unethically as long as the breaches of privacy have been authorized by a duly constituted ethics authority and are the least necessary within that legitimated framework.

Moreover, since private health care providers and consumers are also embedded in a social context—for example, public health care and epidemiological measures are here implicated—the Principle of Legitimate Infringement also entails that if the relevant data in the private sector are demonstrably necessary for appropriate social health care planning, society has the right to access them for such legitimate purposes.

The key condition here, of course, is that of necessity—which introduces the next clause:

2. HIPs have a duty to ensure, insofar as this falls within there area of competence, that

a. only data that are relevant to legitimate research or planning needs are collected;

b. the data that are collected are de-identified or rendered anonymous as much as possible, in keeping with the legitimate aims of the collection;

c. the linkage of data bases can occur only for otherwise legitimate and defensible reasons that do not violate the fundamental rights of the subjects of the records; and

d. only duly authorised persons have access to the relevant data.

This clause identifies the limits within which HIPs may ethically participate in activities that are allowed under Clause D.1. These limits are defined by the Principles of Information-Privacy and Disposition, Legitimate Infringement and of the Least Intrusive Alternative, and they are very strict. There must be a demonstrable need for collecting the data,[lxix] the data must be de-identified or rendered anonymous as much as possible in keeping with the legitimate aims of collecting the data in the first place, and that every effort must be made to make it impossible to link the data bases in which the data are kept except for independently justified legitimate purposes where these purposes are defensible not merely in legal but also in ethical terms, and where the linkage is performed and the linked data are used only by duly authorized persons who are legally bound to confidentiality regarding the relevant data.[lxx]

That is to say, modern technology makes it possible to collect all sorts of data for all sorts of purposes. However, the fact that it is possible to collect data does not entail that ethically speaking they should be collected. This is particularly true in the field of health care, where the special nature of the data and their unique connection to the individuals about whom they are engages fundamental considerations of privacy. At the same time, if society is to be able to meet the health care needs of its members, planning is necessary, and that planning cannot occur unless relevant data are collected. Consequently the collection of data relative to the planning and delivery of health care is ethically legitimate.

However, planning the delivery and structure of health care is not individual- but group-specific. Therefore the data that are collected need not necessarily have identifiers or otherwise be linked to individual persons. It follows that, in order to protect the privacy rights of members of society, the data that are collected should be as de-identified or anonymous as much as possible, in keeping with the legitimate aims of the collection. This of course means that the degree to which this should be the case depends on the aim of collecting the data in the first place. Thus, the data that are collected for the use of health care professionals in order to look after the health care needs of individual patients and are contained in EHRs, should have identifiers and should be linked to the individual subjects of the records. However, the data that are collected and used for health care planning at the policy level need not have identifiers attached to them. Hence the phrase “in keeping with the legitimate aims of the collection.”

The reality, of course, is that once data have been collected and are contained in records that are stored in a data base, the data base can linked to other data bases. This makes it possible to develop profiles for individuals whose data are contained in the otherwise distinct data bases even if the data in the distinct data bases are de-identified or rendered anonymous. A minimum of four distinct data will allow for the re-identification of the individual. This, in turn, raises the possibility of developing profiles that are erroneous simply because the disparate sets of data of the distinct data bases were never intended to be connected into a single profile, and the connections that are made in developing such profiles lie outside of the distinct parameters that determined the collection of the data into the respective data bases in the first place.

Consequently, HIPs have a duty not to participate in data base linkages if the need for such linkages and the conditions under which they are linked cannot be justified in ethically defensible terms—i.e., if it cannot be shown that in the absence of such linage the otherwise legitimate aims of society could not be achieved. This includes linkages that are necessary to engage in a particular kind of health related research. Therefore the claim that such linkage is necessary should be validated by a duly constituted ethics committee to whom the proposed linkage project should be submitted for consideration. Moreover, HIPs have an obligation not to participate in profile developments across data bases that cannot be justified in a similar manner. Finally, HIPs have an obligation to ensure, as best as they are able, that only duly authorised persons have access to the relevant data bases and to the data contained in them.

3. HIPs have a duty to educate the public about the various issues associated with the nature, collection, storage, use, linkage and manipulation of health related data and to make society aware of any problems, dangers, implications or limitations that might reasonably be associated with the collection, storage, use, linkage and manipulation of such data.

This clause extends the duties of HIPs, both individually and as a profession, into the arena of public education. The reason for this is simple. People have a wide variety of disparate opinions about the benefits and dangers of electronic records and about the use to which the data that are contained in them may be put. At the one extreme, there are those who consider electronic health records an infringement of their right to Information Privacy and Disposition; at the other extreme, there are those who think that collecting electronic health data and establishing databases poses no problem.

Not all of these opinions are properly informed or reasoned. Since public opinion strongly determines the political process, this may lead to inappropriate political decisions being made that may have severe effects on society's overall ability to plan and deliver health care. HIPs, because of their unparalleled knowledge and training, are uniquely placed to explain to the public the various issues that are associated with electronic health records. Without such information, society cannot make an informed choice and develop appropriate rules and guidelines, and the Principle of Information Privacy and Disposition might well be applied in an inappropriate fashion and result in a less than optimal health care delivery. Therefore

the fundamental ethical Principles of Beneficence and Non-Malfeasance entail that HIPs have a duty to educate society on these matters.

4. HIPs will refuse to participate in or support practices that violate human rights.

HIPs are embedded not only in the immediate contexts in which they work but also in society at large—and indeed in global society when they are functioning in an interjurisdictional eHealth setting or are providing informatic and related services in the context of outsourcing when this service crosses national boundaries. This gives rise to the general duty that is stated in Clause D.4. This duty is grounded in the Principle of Non-Malfeasance.

More particularly, it is possible to use EHRs and other informatically related items, and to employ informatic tools or practices for purposes other than the planning, maintenance or delivery of health care. While this may be legitimated by the legal framework in which the HIP is operating, it can be ethically unacceptable when it involves the violation of the right of privacy and of the right of integrity of the person as guaranteed by the *Universal Declaration of Human Rights*.[lxxi]

As to privacy, while the issue of privacy has already been addressed in Section **A** of this Handbook, and while the unauthorised use of patient-relative data has also been dealt with, how and why this may relate to other violations of human rights in the context of medical informatics and the role of HIPs was not explicitly considered. Beginning, then, with Directive 95/46 EC of the European Union—which was promulgated in 1995[lxxii] and was replaced in 2016 as Regulation (EU) 2016/679—it stipulates a right to privacy and control.[lxxiii] The right was entrenched as a legal obligation on others by the European Court Ruling C-131/12 of 13 May 2014, which in turn officially recognized that informatic rights in health care are a subspecies of human rights. A similar position was adopted on a global scale by the Organisation for Economic Co-operation and Development in its 2015 document entitled *Health Policy Studies Health Data Governance Privacy, Monitoring and Research*, and on a still more universal scale [lxxiv] was asserted as a fundamental right of all persons in the *Universal Declaration of Human Rights*. Consequently, as a matter of human rights, HIPs should refuse to participate in or support practices that violate the ethics of privacy as spelled out in the *Universal Declaration of Human Rights.* In particular, as was already mentioned above, this applies when doing so would facilitate or enable the violation of the right to integrity of the person and the right not to be subjected to torture or to cruel, inhuman or degrading treatment or punishment.

That is to say, the *Universal Declaration of Human Rights* stipulates as a matter of ethics not only that everyone has the right to privacy, but also the right to integrity of the person and the right not to be subjected to torture or cruel, inhuman or degrading treatment or punishment. These rights, and in particular the latter, can easily be infringed—and indeed sometimes are—by the use of interrogation techniques that are attuned to the health profile of the individual person.[lxxv] Similar remarks apply to the use of EHRs or of data contained in them to develop ethnicity-specific bioweapons.[lxxvi] There may be occasions where, directly or indirectly, HIPs may be involved in such practices because use of, access to

and communication of the relevant records may involve them as informatics professionals. If such were to be the case, the relevant HIPs would be guilty of a human rights violation.

Once again, the point here hinges on the relationship between moral responsibility and complicity. To reiterate what was said before, individuals who are instrumentally involved in the violation of a human right cannot escape responsibility merely because they are not directly and personally engaged in the relevant act. Involvement itself, if it is instrumental, facilitating and enabling, is sufficient to trigger complicity. While the notions of complicity and co-responsibility continue to be clarified mainly in the context of war crimes and crimes against humanity,[lxxvii] the fundamental ethical and legal principles that are here involved are universal and beyond dispute.

Applied to the present context, this means that if HIPs are instrumental to the existence of EHRs, and if they are integrally involved in a process that leads to their misuse then, because of their causal and facilitating role they become complicit in any violation of human rights that might occur. HIPs therefore are ethically bound to refuse participation in any such action—just as soldier have a duty to refuse participation in or to follow the directives of a military structure that violates fundamental ethical principles, and cannot point to the fact that they are following orders or are acting in accordance with an established national protocol as an exculpating factor.[lxxviii]

5. HIPs will be responsible in setting the fee for their services and in their demands for working conditions, benefits, etc.

Professionals—and HIPs are no exception—have a right to appropriate recompense for their services. Sometimes it happens that the professionals are not satisfied with the rate at which they are recompensed, the conditions under which they work or the benefits that they enjoy, and consider taking what might euphemistically be referred to as “job actions.” Such actions are the more successful, the greater their impact on employers, institutions and society at large. From this perspective, HIPs are in an immensely powerful position because they essentially control the data flow in the health care sector. However, when using that power, HIPs should keep in mind their comparative position vis-à-vis other similarly placed professionals in society, and should be guided by the Principles of Beneficence and Non-Malfeasance. In other words, they should be responsible in their demands, and should not knowingly endanger either individual or public welfare through their actions.

In particular, since modern health care relies on EHRs and electronic communication, if the HIPs supply informatic services to a given institution, organization health care facility or the like, and if the latter depend on the HIPs to be able to carry out their own mandate then, then if the HIPs were to withdraw their services entirely the latter would be unable to meet their health care related obligations. Since access to timely, acceptable, and affordable health care of appropriate quality is a human right,[lxxix] this right would be violated if the HIPs whose actions are instrumental for making the fulfilment of this right possible were to withdraw their services entirely. Consequently HIPs have an ethical duty to ensure that appropriate alternatives are in place if they decide to undertake job related actions.

E. Self-regarding duties

HIPs are not only professionals but also moral agents. As such, their major concern should always be to act in an ethically appropriate fashion. Therefore, even in situations that do not involve a clear duty towards others, there may still be duties that HIPs have towards themselves as persons because failing to fulfil such duties may diminish them as moral agents. These, then, are self-regarding duties—duties that HIPs have towards themselves as moral beings. They frame how HIPs situate themselves ethically in the professional world.

1. HIPs have a duty to recognize the limits of their competence,

This clause identifies a self-regarding duty that is grounded in the Principle of Integrity. It is the duty to be aware of what one is and is not qualified to do as a professional. Such awareness can be achieved only if HIPs adopt an attitude of critical self-examination in their professional lives. Failure to be aware of the limits of one's competence may result in misrepresentation of one's qualifications, which would be a violation of the Principle of Integrity.

Further, it may result in HIPs accepting tasks or positions for which they are not qualified, which in turn may mean that they would be unable to perform the tasks that were identified by their employers as integral to the nature of their employment. It is only if HIPs follow this injunction that they can act in a professional appropriate manner in general, and in particular meet the conditions that are set out in clauses **B.4**, **C.2 (e)** and **C.8** of this Code.

2. HIPs have a duty consult when necessary or appropriate.

Clause **E.1** directly leads to the duty that is enunciated in **E.2**. Despite the best of training and conscientious diligence in keeping current with evolving professional standards, HIPs may encounter situations they have never encountered before and where past experience offers little or no guidance. Likewise, they may encounter situations where there are different ways of interpreting or dealing with the matter that faces them and it is unclear which one is appropriate or best. In these and similar circumstances the Principle of Integrity entails that HIPs have a duty to consult with appropriately placed colleagues who may be of assistance in resolving the situation. On such occasions, however, HIPs have a duty to try and obtain permission from those whose privacy would be at issue before doing so. When this is not possible because time is of the essence, and if there are no reasonable grounds to suppose that consultation would be considered unacceptable or inappropriate, they should go ahead and consult. However, they should inform the relevant individuals as soon as is reasonably possible of the fact that

such consultation has occurred. Further, they should always do their best to ensure that all relevant privacy and security consideration that have been enunciated in the previous sections of this Code are observed.

3. HIPs have a duty to maintain competence.

HIPs are hired by employers because they hold themselves out as being qualified and competent to perform the tasks that are identified in the job description for the position in question. It can generally be assumed that unless the HIPs misrepresent their qualifications—which would be a violation of the Principle of Integrity—they will be duly qualified and competent at the point of employment. However, the unspoken assumption that underlies an offer and acceptance of employment is that whoever accepts that employment will not merely be qualified and competent at the point of employment but will maintain that competence for the duration of that employment. Hence the duty that is identified in **E.3.**

However, a further underlying assumption of employment is that if the professional standards for carrying out the tasks that are associated with that position change, and if the tools, techniques or relevant other means for carrying out the tasks that are associated with that position change, those who have accepted employment will upgrade their qualifications so as to be able to perform their tasks in the best possible manner. Therefore, the Principle of Integrity also entails that HIPs not merely have a duty to maintain competence but also to maintain competence in accordance with the evolving standards of the profession.

At the same time, more is involved in maintaining professional competence than having and maintaining appropriate professional qualifications. The fact is that even though HIPs may be professionally competent, they cannot fulfil their obligations in the best possible manner unless they are mentally and physically in a state of health that allows them to function properly. Consequently HIPs also have a duty to do the best they can to achieve and maintain proper mental and physical health, consistent with the roles to which they have committed themselves as professionals. This is not merely a self-regarding duty but also a derivative duty that they owe their employers and those who rely on their professional services.

4. HIPs have a duty to take responsibility for all actions performed by them or under their control or authority.

This duty is again grounded in the Principle of Integrity. To perform a task and then to deny that one has performed it is to lie. That is unethical. Therefore ethical HIPs will always take responsibility for whatever actions they have performed. With due alteration of detail, this also applies to actions that are performed under their control or authority. The reason is simple. Actions performed under their control or authority would not have been performed but for that control or authority, and the individuals who perform the

actions do so only at the HIPs' behest. Therefore while an HIP may not be the individual who actually carried out the task in question, the HIP caries the responsibility for that action or that task having been performed.

5. HIPs have a duty to avoid conflict of interest.

Professionals who accept employment from an agency, institution or individual bind themselves, by accepting that employment, not only to act in the best manner possible but also in the best interests of their employer. However, situations may arise where what is in the best interests of the employer comes into conflict with other obligations that the professional may have or with the professional's own best interests. In such a situation, the professionals would be in a conflict of interest.

HIPs who allow themselves to be caught in a conflict of interest have failed to recognize the truth of the age-old maxim that one cannot serve two masters at once. Inevitably, one set of interests will have to be compromised—and possibly both. A moral outlook that is not sensitive to this fact is an outlook that guarantees moral failure. It is also an outlook that places little value on moral integrity, thereby violating the HIP's duty of moral authenticity—the duty to respect oneself as person. Consequently HIPs have a duty to avoid conflict of interest. This will allow them to function without undue problems as moral agents If a conflict of interest arises or threatens and cannot be avoided, HIPs have a duty to advise their employer or other relevant individuals or parties of this fact and seek appropriate instructions for how to proceed so that they may avoid making ethically indefensible decisions that would undermine their moral standing.

6. HIPs have a duty to give appropriate credit for work done

The professional life of HIPs should be morally authentic: It should be shaped by the values of integrity, honesty and diligence—not only because HIPs owe this to other parties, but because they also owe it to themselves as moral agents. Sometimes the work that HIPs perform is performed directly and solely by the HIPs themselves and in their own person; however, at other times it involves the assistance of others. In such cases, for the HIPs not to acknowledge this assistance constitutes deceit. Ethically speaking, deceit—and the failure to give credit where credit is due is really a form of deceit—is morally reprehensible and should be avoided if one wants to retain "ethically clean hands." It may also harm the other person to whom credit is due by depriving them of the recognition that would advance or consolidate their position, thus violating the Principle of Non-Malfeasance.

7. HIPs have a duty to act with honesty, integrity and diligence.

What is expressed in this clause is merely the summation of what underlies the various clauses in this Code, and of what it is to be an ethically upstanding individual in a professional setting. Hence it requires no further comment or explanation.

F. Duties towards the profession

In general terms, a profession is an association that is controlled by governing body that directs professional behaviour, that sets entry standards and standards of professional competence as well as the ethical rules for its members, and that gives leadership in the field of learning relative to its domain of specialization. Professions tend to be—but are not necessarily—identified and recognized by statute. The reason that HIPs owe the duties that are outlined below to their profession is that it is the profession that really validates the position of HIPs in society.

Perhaps the most important of these duties for HIPs is the first, because it goes to the very ability of Health Informatics to function as a profession.

1. HIPs have a duty to always act in such a fashion as not to bring the profession into disrepute.

When HIPs act in a professional capacity they are not merely acting in their own person, they are also acting as members of the profession of Health Informatics. Inevitably, therefore, how HIPs conduct themselves has repercussions on how the profession is perceived by society. But it may go beyond that: If the profession is perceived as disreputable, it may even lead to its de-certification and disappearance as a profession. However, even if that does not occur, it may result in opportunities of service that would otherwise exist becoming restricted or even closed to the profession and its members. All of this would have negative consequences not only for the profession and its members but also on the planning and delivery of modern health care which increasingly depends on health informatics. Since this would imperil the lives and welfares of member of society, bringing the profession into disrepute would be a clear violation of the Principle of Non-Malfeasance.

2. HIPs have a duty to assist in the development of the highest possible standards of professional competence, to ensure that these standards are publicly known, and to see that they are applied in an impartial and transparent manner.

This duty centres in the fact that as informatics professionals, HIPs have a better sense than anyone else of what constitutes competent professional behaviour. This is reflected in the fact that society relies on HIPs not only when informatic issues are involved in health care delivery and planning, but also when expert witnesses are called upon in evaluating whether a particular HIP has acted according to appropriate standards and within the bounds of competence. While this places HIPs in a position of advantage, it also imposes on them a burden: The Principle of Integrity demands that HIPs exhort and assist their profession to develop the highest standards of competence, so that society may be served in the best possible way. It also entails that HIPs should do their best to ensure that these standards are publicly known, so that society has some understanding of what can (and what cannot) reasonably be expected from individual HIPs and from Health Informatics as a profession.

Finally, it entails that when the situation so demands, HIPs should be willing to see this knowledge and these standards applied impartially (lest the reputation of the profession be brought into disrepute) and in a transparent manner, so that no hint of impropriety attaches to the profession's peer evaluations.

3. HIPs will refrain from impugning the reputation of colleagues but will report to the appropriate authority any unprofessional conduct by a colleague.

Unprofessional conduct harms not only those who are directly affected by it, but also the profession; hence the general duty enunciated in Clause **F.1** not to bring the profession into disrepute. That duty applies directly to each HIP. However, there is a second side to that duty: It is the correlative duty to take appropriate steps when a colleague engages in unprofessional behaviour. This duty is rooted in the Principle of Non-Malfeasance in the following way: Harm can be produced either directly by actually engaging in some sort of activity, or indirectly by refraining from doing something that is mandated. The concept of negligence here finds its basis. When someone is negligent, it is not that the individual has done something but that the individual has failed to do something.

Failing to take appropriate steps when a colleague engages in unprofessional conduct falls into this category. It constitutes negligence. The reason it constitutes negligence is that, as is stated in **F.2**, HIPs have a duty to see that the highest possible standards are applied in an impartial and transparent manner. Therefore HIPs who become aware of unprofessional conduct by colleagues would be negligent if they did not report such behaviour to an appropriate authority. Indeed, not only would they share in the responsibility for any harm that might result from failing to report the conduct, they would actually be endorsing such conduct by their inaction.

Of course, the Principle of Non-Malfeasance also has a corresponding side to it: Unfounded accusations can easily ruin the reputation of a colleague. Therefore HIPs should be careful in making accusations, and should have reasonable grounds before undertaking any actions in this regard. Moreover, the sort of action that is taken by the HIP—for instance, how the unprofessional conduct is brought to the attention of the appropriate authorities, and indeed to whom the conduct is reported—is also ethically important. The Principle of Equality and Justice is here implicated. Everyone has the right to be treated fairly, and

fairness demands not only that HIPs have ;reasonable grounds before undertaking the relevant actions, but also that the actions they choose are commensurate with the issue at hand.

4. HIPs have a duty to assist their colleagues in living up to the highest technical and ethical standards of the profession.

Non-one is perfect. Therefore it sometimes happens that HIPs need help in living up to relevant standards and expectations. If colleagues are not willing to assist each other in this regard, the failure to do so would constitute negligence, and would set the stage for harm to occur in two ways: once to those who fail to receive the proper services because of the inappropriate conduct itself; and once to the individual who, if he or she had been helped, would not have engaged in that inappropriate conduct in the first place.

By the same token, an opportunity for doing good would have been lost. Therefore this clause is based on the Principles of Beneficence and Non-Malfeasance. That is to say, Clause **F.3** enunciated the duty to take appropriate steps when there are reasonable grounds to suppose that a colleague is guilty of unprofessional conduct. Clause **F.4** recognizes that colleagues may need help in living up to the highest professional standards, either in a technical or an ethical sense. The reason this duty is owed the profession is that the reputation of the profession as a whole will suffer if its practitioners do not practice their profession in a uniformly excellent way.

5. HIPs have a duty to promote the understanding, appropriate utilization, and ethical use of health information protocols and technologies, and to advance and further the discipline of Health Informatics.

The profession of Health Informatics is grounded in a discipline that has a tremendous amount to offer to society; however, it cannot fulfil its promise unless society is aware of what it can do. The Principle of Beneficence therefore entails that HIPs owe it to society as well as to their profession to promote a proper understanding of the potential contributions that Health Informatics can make. At the same time, this potential will be undermined if the discipline does not explore new possibilities, extend its horizons and keep up with developments in related areas. Consequently, HIPs should do their best to advance the discipline so as to do their part in making the world a better place.

REFERENCES

[i] http://www.un.org/en/universal-declaration-human-rights/index.html.
[ii] For instance, the *ACM Code of Ethics and Professional Conduct* (https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct)
[iii]In this Handbook, no distinction is made between electronic health records, electronic medical records and electronic patient records. Although that there are considerable differences in their content and detail, all of these records should be handled under the same ethical principles.
[iv] 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.
[v] 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 Kluge E-H W, "Electronic Health Records," *Encyclopedia of Global Bioethics*, available at http://link.springer.com/referenceworkentry/10.1007/978-3-319-05544-2_168-1.
[vi] In what follows, the term 'institution' will be understood as being short for 'institution, organisation or agency'.
[vii] 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.
[viii] IMIA Code of Ethics; available at http://imia-medinfo.org/wp/wp-content/uploads/2015/07/IMIA-Code-of-Ethics-2016.pdf
[ix] *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (C-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.
[x] For discussion of some trends and issues, see WHO *Global Observatory for eHealth* vol. 3-6.

[xi] Public Law 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 11/27/17 at https://www.congress.gov/bill/114th-congress/house-bill/2048/text .

[xii] 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.

[xiii] For a reflection of this, see *Universal Declaration of Human Rights*, Article 1, 18, etc.; available at http://www.un.org/en/universal-declaration-human-rights/index.html.

[xiv] For a reflection of this, see *Universal Declaration of Human Rights*, Articles 2, 6 and 7; available at http://www.un.org/en/universal-declaration-human-rights/index.html.

[xv] For a reflection of the Principle in the laws of some countries, see Argentina, Penal Code Articles 106-108; Belgium, *Criminal Code* article 422; France, *Criminal Code* Art 223-6; Germany, *Criminal Code* § 323c; Russia, *Criminal Code*, Article 125.

[xvi] See *Universal Declaration of Human Rights* Articles 3-5.

[xvii] This Principle finds legal reflection in the maxim *lex non cogit ad impossibilia*. For a reflection, see India, *Contract Act* 1972 s. 56. The principle is reflected in Commonwealth law as the Doctrine of Impossibility, and finds similar reflection in Japanese and Korean law, as well as in most other jurisdictions. It goes back as far as Justinian, (*Digest* 50. 18. 185) and is generally accepted in international law even when evaluating performance of treaty obligations. See Reuter P. *Introduction au droit de traités* (Paris, 1985), pp. 152-157.

[xviii] While not explicitly stated as such in most jurisdictions, this principle is reflected in most countries' laws that deal with negligence and duty of care.

[xix] The term 'framework' is used in this and subsequent contexts relative to the functioning of the technical systems in which EHRs are developed, stored handled, manipulated, commutated etc. in order to indicate that more than technical issues are here at stake. The actual operation of such an informatic system involves non-technical and non-material components that include handling protocols, security and quality measures etc. that have person-focused parameters.

[xx] For relevant informatics related standards, see ISO/TC 215 - Health informatics; available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=54960.

[xxi] Bayles, M. *Professional Ethics*, Wadsworth, 1989; Freidson E. *Professional Powers: A Study of the Institutionalization of Formal Knowledge*, University of Chicago Press, 198; Parsons, T. *Essays in Sociological Theory* Glencoe, Ill. : Free Press, 1954.

[xxii] On a global scale, the high-water mark of this development was the release of the Flexner Report in 1910; see Flexner (1910, 1912).

[xxiii] E.g., in England the Nurses Registration Act of 1919 established nursing as a registered profession; in France the government issued a national diploma for nursing in 1922; in India Madras State formed the first registration council in 1926 and the Indian Nursing Council was established in 1947; in Japan nurses were regulated as a profession by the Nurses Rules of 1915 and the N he National Healthcare Act enacted in 1942 regulated public health nurses, midwives and nurses as healthcare professionals along with medical doctors and dentists.

[xxiv] Cf. S. Breakey, I.B. Corless, N.L. Meedzan, P.K. Nicholas. *Global Health Nursing in the 21st Century* (Springer, 2015) Chapter 3, "A Foundation for Global Health", p. 43.

[xxv] See the 1231 law of Frederic II of Hohenstaufen which, in article 45, stated that 'In view of the severe consequences and the irremediable harm that may result when inexperienced physicians engage in practice, we order that henceforth no-one may dare to practice medicine under the title of physician if he has not previously been approved in an open disputation by the professors of the University of Salerno.'

[xxvi] For instance, the American Medical Informatics Association, the Sociedade Brasileira de Informática em Saúde, the Indian Association for Medical Informatics, the Japan Association for Medical Informatics, etc.

[xxvii] Or their duly empowered substitute decision makers.

[xxviii] They also derive from the relationship between HIPs and the institutions, employers and agencies with whom they are associated in a professional capacity. For more on this, see Section C, *infra*.

[xxix] World Medical Association, *International Code of Medical Ethics*, available at http://www.wma.net/en/30publications/10policies/c8/.

[xxx] See p. 9, supra.

[xxxi] World Medical Association, *International Code of Medical Ethics*, available at http://www.wma.net/en/30publications/10policies/c8/.
[xxxii] Cf. p. 5, *supra*.
[xxxiii] Oxford English Dictionary, 'complicity; at https://en.oxforddictionaries.com/definition/complicity
[xxxiv] It may even involve the individual's sex Cf. Nader Said-Foqahaa, "Arab Women: Duality of Deprivation in Decision-making under Patriarchal Authority", *Journal of Women of the Middle East and the Islamic World* 9 (2011) 234–2; "World Report 2013 - Saudi Arabia". 2013. Human Rights Watch, retrieved 23,01, 2017 from https://www.hrw.org/world-report/2013/country-chapters/saudi-arabia.
[xxxv] Cf. Kuther, T.L. 2003. "Medical Decision Making and Minors: Issues of Consent and Assent". *Adolescence* 38, 150: 343–58; Whitty-Rogers, Joanne et al. 2009. "Working with Children in End-of--Life Decision Making". *Nursing Ethics* 16, 6: 743–58
[xxxvi]For instance, Canada. See *A.C. v. Manitoba (Director of Child and Family Services)*, 2009 SCC 30, [2009] 2 S.C.R. 181.
[xxxvii] Further, the meanings of the terms 'competence' and 'capacity' may vary even within a given jurisdiction. Thus, in some jurisdictions 'competence' refers to the legal ability to understand and make decisions and 'capacity' refers to a medical finding of decision making capability, whereas in other jurisdictions the reverse holds true. In this document the two terms are used interchangeably and are understood as referring of the ability to cognitively understand the nature of a given situation, the nature and implications of any treatment options that are offered, and the ability to make a rational decision that is based on that understanding.
[xxxviii] Strictly speaking, this is not quite correct. The law distinguishes between natural persons and legal or juridical persons. Natural persons are living members of the *species homo sapiens*; legal persons are entities like corporations, social agencies and the like which are imbued by law with rights and duties. Cf. Kelsen H. (1960/1967). *Pure Theory of Law*, M. Knight, trans., Berkeley: University of California Press. However, since legal or juridical persons are not biological entities, they cannot and do not have EHRs. Consequently they play no role in considerations dealing with the ethics of EHRs and the rights and duties of HIPs.
[xxxix] Cf. Buchanan, Allen E., and Dan W. Brock. 1989. *Deciding for Others: The Ethics of Surrogate Decision-Making*. Cambridge: Cambridge University Press.
[xl] Okamura, H., Yosuke, U., Sasako, M., Eguchi, K., and Kakizoe, T. 1998. Guidelines for telling the truth to cancer patients. Japanese Journal of Oncology. 28(1): 1-4; Marshall, P.A. 2008. Cultural competence and informed consent in international health research. Cambridge Quarterly of Healthcare Ethics. 17: 206-15; Kaufert, J.M. and O'Neil, J.D. 1991. Culture, power and informed consent: the impact of Aboriginal health interpreters on decision-making. In Social Science Perspectives on Medical Ethics. Weisz, ed. University of Pennsylvania Press; Ho, A. 2008. Relational autonomy or undue pressure? Family's role in medical decision-making. Scandinavian Journal of Caring Sciences. 22: 129-135.
[xli] The reason HIPs only have a duty to maximize the probability is that, as was pointed out above, except for a Vernam cipher code, there can be no guarantee that such measures will be 100% successful in all cases. Such codes are unusable in health care because it would make it impossible to deliver health care in a timely fashion.
[xlii]William Herbert Page W.H. The Development of the Doctrine of Impossibility of Performance. *Michigan Law Review* Vol. 18, No. 7 (May, 1920), pp. 589-614.For an international reflection of this principle, see *Lala Shyamlal Jain Ship Breaking ... vs State Of West Bengal And Anr*. on 26 June, 2004
[xliii] With due alteration of detail, similar remarks apply to duly empowered patient substitute decision makers
[xliv] Cf. Nelson, GS. Practical Implications of Sharing Data: A Primer on Data Privacy, Anonymization, and De-Identification. SAS Global Forums April 26-29 | Dallas, TX) *Proceedings*, 1884-2015; Landi, W and Rao, RB. Secure De-identification and Re-identification. *AMIA Annu Symp Proc*. 2003; 2003: 905
[xlv] Cf. Kluge, The Physician-Patient Relationship in eHealth and Telemedicine: An Ethical Conundrum. *Proceedings of the International Conference on E-Commerce*, Lisbon, Portugal 17-19 July 2014; accessed 21/02/17 at http://www.iadisportal.org/ec-2014-proceedings .
[xlvi] For more on this, see the discussion of "Duties towards Institutions, Employers and Agencies," *infra.*
[xlvii] For more on this, see the discussion of "Duties towards Institutions, Employers and Agencies," *infra*.
[xlviii] For what constitutes "qualified and authorized researchers," see Loue, S. *Textbook of Research Ethics*:. *Research Ethics.* Kluwer, 2000; *A Handbook of Principles and Procedures*, available at http://www.glos.ac.uk/docs/download/Research/handbook-of-principles-and-procedures.pdf.

[xlix] A legacy system is informatic technology, computer system, or application programme that has been superseded by more current technology, programmes or systems.
[l] Replacing or updating legacy systems may not always be necessary (or even appropriate). See Lamb, J. (June 2008). "Legacy systems continue to have a place in the enterprise". *Computer Weekly*; retrieved 31/01/2017 at http://www.computerweekly.com/feature/Legacy-systems-continue-to-have-a-place-in-the-enterprise .
[li] *Cf*. Bisbal, J.; Lawless, D.; Wu, B.; Grimson, J. (1999). "Legacy Information Systems: Issues and Directions". IEEE Software. 16: 103–111. doi:10.1109/52.795108 ; Hein, A.M (2014), How to Assess Heritage Systems in the Early Phases?, 6th International Systems & Concurrent Engineering for Space Applications Conference 2014, ESA.
[lii] Juridically, corporations are considered persons. See United Nations (2011*), Draft Articles on the Responsibility of International Organizations, with Commentaries*, retrieved February-3-17 from http://legal.un.org/ilc/texts/instruments/english/commentaries/9_11_2011.pdf . See also Waite and Kennedy v Germany, Merits, App No 26083/94, ECHR 1999-I, [1999] ECHR 13, (2000) 30 EHRR 261, (1999) 118 ILR 121, IHRL 3200 (ECHR 1999), 18th February 1999, European Court of Human Rights [ECtHR, Grand Chamber]; Matthews v. United Kingdom, App. No. 24833/94, 28 Eur. H.R. Rep. 361 (1999).
[liii] World Medical Association, *International Code of Medical Ethics*; accessed Thursday, February-02-17 at http://www.wma.net/en/30publications/10policies/c8/index.html.pdf?print-media-type&footer-right=%5Bpage%5D/%5BtoPage
[liv] Cf. OASIS SOA Reference Model (SOA-RM) TC, # 2; accessed 2017-02-14 at https://www.oasis-open.org/committees/soa-rm/faq.php .
[lv] See the Principle of Information Privacy and Disposition and the discussion in *Section A. Subject-Centred Duties* above.
[lvi] See note 49, *supra*.
[lvii] See Section A, *supra*.
[lviii] See Section B, *supra*.
[lix] See Section D, *infra*.
[lx] See Section F, *infra*.
[lxi] Commission of Inquiry into the Methods of Investigation of the General Security Service Regarding Hostile Terrorist Activity, available at http://www.hamoked.org/files/2012/115020_eng.pdf . See also Farrell, M. *The Prohibition of Torture in Exceptional Circumstances.* Cambridge University Press, Aug 29, 2013.
[lxii] United Nations General Assembly, *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*, available at http://www.ohchr.org/Documents/ProfessionalInterest/cat.pdf .
[lxiii] See p. 18, *supra*.
[lxiv] See Clause C.1, *supra*.
[lxv] See the discussion under C.1 *supra*.
[lxvi] European Commission (2008) *Data protection and privacy ethical guidelines*; available at http://ec.europa.eu/research/participants/data/ref/fp7/89827/privacy_en.pdf.
[lxvii] This Principle in law goes back as far as Justinian, *Digest* 50. 18. 185, and is generally accepted in international law even in evaluating performance of treaty obligations. See Reuter, P. *Introduction au droit de traités (*Paris, 1985), pp. 152-157.
[lxviii] European Commission, *Towards a European Policy on Open Access*; accessed 17/05/17 at https://erc.europa.eu/sites/default/files/content/pages/pdf/Daniel_Spichtinger.pdf
[lxix] This clause complements Clause A.2 of the *Code*.
[lxx] This Clause complements Clause A.10 of the *Code*.
[lxxi]United Nations, *Universal Declaration of Human Rights*; available at http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf
[lxxii] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[lxxiii] Parliament of Europe. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

[lxxiv] OECD (2015), *Health Policy Studies Health Data Governance Privacy, Monitoring and Research*. OECD Health Policy Studies, OECD Publishing, Paris.
[lxxv] See notes 62 and 63, *supra*.
[lxxvi] "Preventing the use of biological and chemical weapons: 80 years on," Official Statement by Jacques Forster, vice-president of the ICRC, 10-06-2005; accessed 25/04/2017 at https://www.icrc.org/eng/resources/documents/statement/gas-protocol-100605.htm
[lxxvii] 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.
[lxxviii] Nuremberg Trials. "State Parties / Signatories: Geneva Conventions of 12 August 1949". International Humanitarian Law. International Committee of the Red Cross.
[lxxix] World Health Organization, "Health and human rights" Fact sheet N°32 (December 2015); accessed 4/24/17 at http://www.who.int/mediacentre/factsheets/fs323/en/ .

Glossary

Code of Ethics: collection of principles and rules that govern the ethical conduct of groups of individuals.

confidentiality: the duty to respect or accede to and honour the privacy concerns of the subject of a record.

conflict of interest: a situation in which two or more concerns or duties of an individual are incompatible.

data: raw, uninterpreted facts captured according to some agreed-on-standard.

Doctrine of Emergency: also called the D*octrine of Imminent Peril*. The doctrine assumes that when someone is in imminent danger and unable to give informed consent to treatment then—unless there is an advance directive specific to the case or a duly empowered substitute decision maker is reasonably available—the physician or health care professional may provide what would otherwise be standard treatment in that situation without consent.

duty: correlative of right: a task that someone one must perform if the condition under which the duty holds is realized. Duties differ fundamentally from rights in that rights allow right holders to exercise their discretion about whether to exercise them. When the condition under which a duty holds is realized, the individual whose duty it is has no choice but must carry out the relevant task.

eHealth: the use of electronic information and communication technology to provide clinical health care from a distance.

EHR: In this document, 'EHR' stand for 'Electronic Health Record'. It refers to any electronic health record that contains patient-specific health related data, no matter where it is stored. It therefor includes office or clinic-based electronic health records as well as those held by institutions or organizations, or even by patients themselves as well as records that are stored distributedly in the cloud or on a specific instrument, device or server. The trm is therefore understood as inclusive of Electronic Patient Records and Electronic Medical |Record.

ethical principle: basic or fundamental rule that governs moral conduct in a society and the relationship between individuals.

fiduciary: 'Fiduciary' is a standard ethical and legal term that describes a relationship of trust between a trustee and a beneficiary. However, it involves more than trust. The trustee has the obligation to always act in the best interest of the beneficiary even in the absence of specific directions. The trustee also has a duty not to allow personal interests to conflict with the duty towards the beneficiary.

HCP: In this document, 'HCP' is an abbreviation for 'Health Care Professional'. The term refers, inclusively, to professionals who are directly or indirectly engaged in the delivery of health care such as physicians, nurses and therapists and is inclusive of pharmacists, health care researchers and individuals who plan and manage the delivery of health care. In some jurisdiction chiropractors, osteopaths as well as practitioners in acupuncture, Ayurveda, herbalism, homeopathy, naturopathy, Siddha medicine, traditional Chinese medicine, traditional Korean medicine and Unan may also be recognized as health care professionals.

HIP: In this document, 'HIP' is an abbreviation for 'Health Informatics Professional'. The term refers to individuals who are professionally active in the design, development, adoption and application of information technology in healthcare services delivery, management and planning.

information: data that have been processed, interpreted, organized, or structured according to some standard; data-in-relation.

informed consent: the permission to accept or reject an intervention or action. Informed consent obtains only when it is given by a competent individual on the basis of having been advised and having understood all relevant information about that action or intervention.

institution: any formally organized administrative structure or system. An institution may be physically localized in a building or set of buildings, or may be physically distributed and located in distinct locations.

linkage: the process of connecting different records or parts of records so that the data contained in them can be interrelated; connecting data that refer to the same entity across different data sources.

mHealth: the use of mobile electronic communication devices to provide clinical health care at a distance.

privacy: the right to control the collection, storage, access, use, manipulation and communication of information about oneself.

right: correlative of duty: a justified claim that may be exorcized at the discretion of the right holder when the enabling condition is met.

telemedicine: he use of telecommunication and information technology to provide clinical health care from a distance.