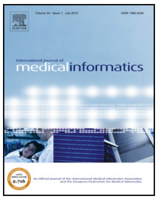
International Journal of Medical Informatics 97 (2017) 261–265

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.ijmijournal.com



Health Information Professionals in a Global eHealth World: Ethical and legal arguments for the international certification and accreditation of health information professionals

Eike-Henner W. Kluge

IMIA (SiHIS) and University of Victoria, Canada

ARTICLE INFO

Article history:
Received 14 June 2016
Received in revised form 19 October 2016
Accepted 29 October 2016

Keywords:
eHealth
Ethics
Health information professionals
IMIA code of ethics
Certification

ABSTRACT

Background: Issues such as privacy, security, quality, etc. have received considerable attention in discussions of eHealth, mHealth and pHealth. However, comparatively little attention has been paid to the fact that these methods of delivering health care situate Health Information Professionals (HIPs) in an ethical context that is importantly different from that of traditional health care because they assign a fiduciary role to HIPs that they did not have before, their previous technical involvement notwithstanding. Even less attention has been paid to the fact that when these methods of health care delivery are interjurisdictional, they situate HIPs in an ethical fabric that does not exist in the intra-jurisdictional setting.

Method: Privacy and other informatic patient rights in the context of traditional health care are identified and the role that HIPs play in this connection is analysed and distinguished from the role HIPs play in eHealth in order to determine whether the 2002 IMIA Code of Ethics provides sufficient guidance for HIPs in eHealth and associated settings. The position of inter-jurisdictional corporate eHealth providers is also touched upon.

Results: It is found that in eHealth, mHealth and pHealth the ethical and legal position of HIPs differs importantly from that in traditional technologically-assisted health care because HIPs have fiduciary obligations they did not have before. It is also found that the 2002 IMIA Code of Ethics, which provides the framework for the codes of ethics that are promulgated by its various member organizations, provides insufficient guidance for dealing with issues that arise in this connection because they do not acknowledge this important change. It is also found that interjurisdictional eHealth etc. raises new ethical and legal issues for the corporate sector that transcend contractual arrangements.

Conclusion: The 2002 IMIA Code of Ethics should be revised and updated to provide guidance for HIPs who are engaged in eHealth and related methods of health care delivery, and to provide a model for a corresponding up-to-date revision of the ethical guidelines that are promulgated by IMIA's member organizations. Similar steps should be taken in the corporate sector so that the ethical rules that govern the working environment of HIPs in the eHealth setting will not pose ethical and professional problems. A possible solution in terms of accreditation and certification is outlined.

The transfer of technology from one domain to another often raises ethical issues that ideally should be identified, explored and addressed before the transfer is initiated. The reason is simple. Different domains of application are situated differently in the social matrix. Therefore even when technically the same issues are at stake, how they should be handled may be quite different because of this difference in social embedding. Simply to transfer the technology and trust to the ingenuity of technical experts to solve these problems is to go forward in the belief that ethical solutions are one-size-fits-all and, more importantly, that technical solutions are answers to ethical problems. As past experience has shown—the transfer of genetic technology from plant and animal husbandry to human medicine provides a glaring example—this belief is not entirely warranted.

eHealth, mHealth and pHealth are quintessential paradigms of technology transfer. In their case, the electronic data collection, transmission, analysis, storage and manipulation technology that had originally been developed for scientific, commercial and internet-related purposes is used to deliver health care-at-distance

E-mail address: ekluge@uvic.ca

http://dx.doi.org/10.1016/j.ijmedinf.2016.10.020
1386-5056/© 2016 Elsevier Ireland Ltd. All rights reserved.

without direct interpersonal contact between health care providers and patients. At first glance, this transfer does not require a fundamental reassessment of the ethical status of individuals who are professionally active in the design, development, adoption or application of IT-based health information systems and in the collection, handling, analysis, storage, linkage, use, manipulation or communication of health information either in an administrative or technical capacity—in short, of health information professionals (HIPs). Privacy, security and confidentiality—issues that are integral to these new methods of health care delivery—had already arisen with the introduction of electronic health records (EHRs). [1–6] Likewise, the issues that are associated with electronic communication and transmission technologies have been extensively canvassed and discussed [7–26]; and even the problem of legacy systems had already been identified as far back as the 1990s [27–30]. Further, the competence and knowledgeability of HIPs regarding technical and ethical standards had been a matter of concern from the beginning [31–33]. Even ethical concerns over the use of the internet in providing health information had surfaced early on [34], and IMIA took the lead in dealing with these and related ethical matters as they concern HIPs by promulgating its Code of Ethics in 2002.[35]However, treatments of these new methods of health care delivery have essentially been silent about the fact that the introduction of eHealth, mHealth and pHealth has resulted in fundamental change in the HIP's professional ethical standing.

In a sense, there have been exceptions. For example, in 2013 the World Health Assembly (WHA)—the decision-making body of World Health Organization—suggested that there was a need for overall standardization of eHealth systems and for the development of an integrated and ethically sound eHealth infrastructure, that it was important to develop and institute some means of proper ethical governance, and that this extended even to such things as the operation of health-related global top-level internet domain names including "health". [36] The WHA further highlighted the need for "devising assessment methodologies" for the technical parameters and devices that are used in eHealth, and suggested that it would be appropriate to "further" ethical standards "through diffusion of guidelines." However, it made no mention of the fact that eHealth and associated delivery modalities situate HIPs in a fundamentally new way in health care delivery, and it was silent on the need for ethical certification of eHealth providers and health information professionals in order to ensure uniformity; nor did it mention the issue of ethical standards for outsourcing eHealth services or when eHealth corporations act across national boundaries. It also did not touch on the issues of liability, of venues for bringing and settling relevant actions, etc. Not surprisingly, therefore, the question of who should function as an authority for deciding these issues and of methods of enforcement was also not addressed. Therefore while the WHA resolution went some way towards outlining issues that emerge when eHealth functions as global method of delivering health care, it did not provide a conceptually and ethically integrated answer to where HIPs stand ethically in this connection.

What follows is an attempt to outline why and how eHealth, mHealth and pHealth have resulted in a fundamental change in the ethical standing of HIPs, and to make some suggestions about how this should be reflected in a revision of the 2002 IMIA Code of Ethics. It also sketches how all of this may appropriately be acknowledged by introducing or adjusting international certification requirements for HIPs. The focus of the discussion will be eHealth but, with due alteration of detail, similar considerations apply to mHealth and pHealth.

To set the stage, it may be appropriate to briefly highlight how eHealth differs from traditional health care and what this means for the status of HIPs. The fundamental difference between the two approaches for delivering health care lies in the fact that traditional health care involves the direct and personal interaction between health care professionals (HCPs) and patients, which in turn establishes a fiduciary relationship between the former and the latter. Of course, in one way or another, patient records have always played an important role in fulfilling this fiduciary duty [37,38], and the introduction of EHRs did not change this [39]. However the records, whether paper or electronic, were never integral to the inception of the fiduciary relationship itself. That was grounded in the direct physician-patient interaction. The records were merely tools—important tools, to be sure, but tools nevertheless. And while the quality of health care has been tremendously improved by the advent of electronic diagnosing, data gathering and manipulation technology, etc. and while the professional-patient interaction has been facilitated by the advent of electronic communication technologies, none of this affected the primacy of direct and interpersonal professional-patient interaction as grounding the relationship itself. Moreover, the role of health information professionals in all of this was that of technical assistants who played a facilitating role, but they were never integral to the establishment of the relationship itself.

In eHealth all of this underwent a fundamental restructuring. The fiduciary physician-patient relationship can no longer be grounded in the direct professional-patient interaction because the very nature of physician-patient interaction has changed. Direct and interpersonal contact has been replaced by electronically mediated contact, and EHRs—which hitherto had been pragmatic tools that could in principle be dispensed with—became an integral feature not merely of the encounter itself but of the very conduct of health care, effectively assuming the role of patient analogues in the health care interaction. [39]

With this, the role of HIPs changed from that of supportive technical players in a framework that was rooted in the physician-patient encounter to that of operant facilitators and interfaces between health care institutions, physicians and patients. As a result, the whole obligation structure that had previously attached primarily to HCPs and institutions and had only incidentally extended to HIPs came to include HIPs in a direct manner. They now acquired a fiduciary role they had not had before except, if at all, in an accidental sense.

To highlight what this means for HIPs it may be useful to focus on privacy and confidentiality as a particular example. Privacy and confidentiality concerns are as old as Hippocrates. They have been addressed in codes of ethics ever since such codes have existed, and have received special attention with the advent of electronic data gathering, communication, storage and manipulation technology and with the development of EHRs themselves. Thus, in 1995 the European Union issued its Data Directive 95/46 EC. [40] It subsequently updated this in 2012 with a new Regulation for the protection of data rights, and the latter replaced the previous Directive in 2016 as Regulation (EU) 2016/679. [41] Likewise, in 2015 the OECD released its Health Policy Studies Health Data Governance Privacy, Monitoring and Research [42] which considered these issues on a global scale. Some of the ethical and legal issues that are here involved were spelled out explicitly in the European Court Ruling C-131/12 of 13 May 2014[43] which stipulated that controllers, operators, users, holders etc. of personal information are not owners but custodians of that information. In fact, it was recognized that informatic rights in health care are a subspecies of human rights, [43,31] and that whoever is involved in their development, communication, maintenance and manipulation has a fiduciary obligation towards the subjects of the relevant records. [44]

From an ethical perspective, how this affects HIPs who are engaged in eHealth is not merely a matter of juridical decisions and considerations but is grounded in the role of HIPs in eHealth and in the relationship between moral responsibility and complicity.

That is to say, reason suggests that persons who are instrumentally involved in the violation of a right cannot escape responsibility merely because they are not directly and personally engaged in the 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 [45,46], the fundamental ethical and legal principles that are here involved are universal and beyond dispute.

This means that if HIPs are instrumental to the existence and use of EHRs as material entities—and they are—and if they are integrally involved in the very existence and process of eHealth as an enterprise—and they are—then through their causal and facilitating role they become complicit in any violation of human rights that might occur in the conduct of eHealth. HIPs therefore have a fiduciary duty towards the patients who enter eHealth, and must do their best to ensure that the informatic aspects of the eHealth systems within which they work are appropriately structured so as to safeguard the informatic and other human rights of the patients. Moreover, they are ethically bound to refuse participation in a system that violates these human rights—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 [46].

In other words, given their absolutely pivotal role in the construction, maintenance and operation of eHealth, HIPs not only have a duty towards their employers and health care providers—an obligation that is usually spelled out in contractual terms—but have a fiduciary obligation towards the patients who are at the centre of eHealth itself, and to provide technical measures that safeguard the privacy and confidentiality of the patients' records. Equally as important, however—given that health care is involved, and that the delivery of such care through eHealth is impossible without the active engagement of HIPs—this fiduciary relationship also includes the duty to ensure the accessibility, usability, integrity and security of these records and the functioning of the communication systems and devices on which eHealth relies and without which eHealth itself would not be possible. While previously such duties existed separately and distinctly and were not fiduciary in nature, they became fiduciary with eHealth precisely because of the fundamentally causal and enabling nature of the HIPs' actions.

At the same time, it is important note that as matter of fundamental ethics and law, the strength of one's ethical and legal obligations is conditioned by the Principle of Impossibility. One cannot have a duty to do the impossible. To put it differently, "ought" implies "can."[47] Nothing can guarantee EHR privacy in an eHealth world. The reason is simple. EHRs are integral to the very possibility of eHealth because eHealth requires their communication. As soon as they are communicated, however—and especially if they are communicated through the internet—their privacy is functionally determined by the measures that are put in place to ensure the security of the communication processes and storage devices, and by the strength of their encryption. However, as Shannon proved in 1949, any encryption can be broken, the sole exception being a record that is encrypted using a Vernam cipher or one-time pad [48]. Such encryption, however, would make EHRs practically unusable in eHealth, which relies on speedy and repeated communication. The best one can do is make the decryption of EHRs extremely difficult and expensive. And even this may not deter someone who has huge amounts of computing power, and it may become as good as irrelevant with the continuing evolution of quantum computing.

Likewise, there are limits on the obligation that HIPs have to provide for security, integrity and accessibility in eHealth. As was said a moment ago, one cannot have a duty to do the impossible. [48] Therefore the strength of these obligations is conditioned by the technology and the resources that are available. Further, they are conditioned by the balance that must be struck between what is possible and what is workable. When the former exceeds the latter, the fiduciary duty to ensure the best that is possible can be mitigated by a corresponding duty to ensure that patients who enter the system are aware of and have given informed consent to its limitations. Therefore while the fiduciary duties that have arisen for HIPs with eHealth are profound and even game-changing, they are subject to justifiable conditions.

What follows, therefore, should be seen as an attempt to flesh out the ethical aspects of this new development and of the WHA's suggestions by sketching how they could be reflected in a globally valid accreditation and certification system for HIPs under the lead of an augmented IMIA Code of Ethics.

The task itself has two sides: first, as a matter of formal ethical requirement, it must do justice to the fundamental changes that have resulted from the expanded role of HIPs in eHealth; second, it must acknowledge the corporate and interjurisdictional realities of eHealth as a business.

As to the first, it is important to note as a preliminary point that the general provisions of the 2002 IMIA Code of Ethics for Health Information Professionals [35] have not been rendered obsolete by eHealth because the underlying principles of health information ethics have not changed, as neither have the general rules of ethics for HIPs. What has changed since the Code's initial promulgation is the role of HIPs because of the extension of their operational framework with eHealth and the introduction of cloud-based and similar record storage and manipulation activities. Therefore what is required is an extension of the 2002 framework for implementing the principles so as to accommodate the new aspects of their role in this new setting.

A first step in doing so would be for IMIA to make appropriate revisions to its 2002 Code to more clearly reflect the expanded responsibilities of HIPs in this new and global context, with an eye towards developing standards of accreditation and certification. Such revisions could include the requirement that HIPs be familiar with any relevant differences in privacy and related informatic provisions in the different domains-of-operation of the corporations by whom they are employed, that HIPs show evidence of currency in this regard through re-certification on a regular basis, and that HIPs show evidence of technical proficiency. The revised code could then form the basis of a globally accepted accreditation and certification protocol for HIPs who wish to work in eHealth in an interjurisdictional setting. The accreditation and certification itself would lie in the hands of a separate and independent branch of IMIA, possibly on the model of an international agency with close ties to WHO as an ex officio and sponsoring member [49]. In order to take advantage of the expertise and to take into account the perspectives of different informatics organization and agencies, the working membership of this agency could be drawn from such organizations as the national health informatics associations who are members of IMIA as well as from such agencies as the Council of European Professional Informatics Societies, the Asia-Pacific Association of Medical Informatics, the International Association of Privacy Professionals, the Association of Computing Machinery, the Healthcare Information and Management Systems Society, the International Conference of Data Protection and Privacy Commissioners, and related international organizations.

The function of this agency would be threefold: to set international standards of technical proficiency and ethical understanding for HIPs, to certify health information professionals as meeting these standards, and to monitor and adjudicate profession-related issues from an inter-jurisdictional perspective. The technical certification process could be based on the models that have been developed by such countries as Belgium [50], Canada [51] or other jurisdictions and by IMIA associated agencies that have developed certification programs for their members. It would have both a technical and an administrative competence focus, and would be regularly updated as the technology evolves and administrative parameters change in the international setting. Ethical understanding and competence would an integral part of the required skill-set necessary for certification. Sufficiency and competence in this regard would be measured with reference to the amended IMIA Code of Ethics for Health Informatics Professionals. In order to ensure continued competence as the international context of eHealth evolves and develops, certification would be on a limited-time basis and would require evidence of maintenance-of-competence similar to the model that exists for physicians and other health care professionals in many jurisdictions [52]. Certification would be a fee item, which latter would fund the operation of the certification structure itself.

With due alteration of detail—and this would address the second task—similar provisions could be developed for the corporate sector. Central issues in this connection would the establishment of and adherence to standards of privacy, ownership, security, access, etc. as grounded in the basic principles of informatic ethics as outlined in the revised IMIA Code. Since the focus of this discussion is not the corporate framework of eHealth but the ethical issues that face HIPs in the eHealth setting, it suffice to sketch how this could be achieved. Briefly, it could be accomplished by establishing an international body along the lines of the United Nations Commission on International Trade Law (UNCITRAL), [53] where this body would function as guarantor of the ethical status of eHealth corporations. Countries that allow eHealth corporations to function—and it would be expected that, because of the WHO affiliation, this would ultimately include all WHO members[49]—would then permit only such guaranteed eHealth corporations to offer their services. One of the major conditions of certification for eHealth corporations and similar service providers would be that they employ only HIPs who have been certified relative to the provisions set out in the previous paragraphs. That would go a long way towards ensuring the consistency of operation that had been called for by WHA in its 2013 Resolution. Beyond its licensing function, this body could also constitute a venue for informatic-related complaints on the model of UNCITRAL or the European Court of Justice, and would have adjudication and arbitration powers. This would be in keeping with the WHA's recommendation that there should be some means of ensuring adherence to the relevant standards.

Because of its WHO affiliation, the adjudicative body would be juridically independent and its evaluations would focus solely on whether a particular action (or lack of action) was in keeping with the privacy and competence provisions etc. outlined in the revised IMIA Code and would be grounded in human rights, rather than merely being in keeping with a particular set of laws or national treaties. Its operation would therefore be largely impartial in the sense that its decisions would essentially be socioculturally and juridically neutral. Moreover, its functioning would be transparent in that its operation would not be in secret but follow the pattern of adjudicative sessions conducted by the European Court of Justice [54] as adjusted to the internationally more extended practice of the UNCITRAL Commission. [55] Finally, it would accessible in the sense that, in principle, any national subscriber or any user of eHealth care could bring an action. The result of a negative decision by this body would result in the withdrawal of the certification of the impugned party. Since under the present proposal certification would be a condition for HIPs operating in an interjurisdictional context, and since eHealth and health information corporations who function interjurisdictionally would employ only certified HIPs and, finally, since subscribing countries would only allow certified corporations to provide their services, the revocation of certification would have obvious implications.

As a method of providing health care in a global world, eHealth has changed the ethical picture not merely in medical but also in informatic terms. In both instances, the interjurisdictional and inter-cultural context has added ethical parameters that did not exist before but that require clarification and resolution if purely economic interests are not to dominate and trump what ultimately are human informatic rights. HIPs are integrally involved in the very existence and functioning of eHealth, and eHealth and health information corporations are steadily increasing their interjurisdictional footprints. It is therefore advisable that some method of accreditation, certification and adjudication for the professionals and the corporations be devised lest privacy and related informatic rights suffer piecemeal dismemberment and become the victims of inattention; and, just as importantly, lest inappropriate informatic actions undermine the nature and quality of the health care that is provided in eHealth. The proposed certification would differ from what is currently provided by institutions, associations and agencies in various jurisdictions in that it would be grounded in the ethical principles that underlie the treatment of health information itself as these are outlined in the IMIA Code of Ethics and which, with due alteration of detail, are applicable both to health informatics professionals as well as health care providers and corporations [39]. If the proposal just sketched was fleshed out and implemented, the result would provide for a process that would transcend national boundaries and put eHealth, mHealth and related methods of health care delivery on a firm ethical footing that recognized their unique nature and the special position of HIPs in their deployment and design.

Author's contribution

I am the sole author of this paper.

Conflict of interest

I have no conflict of interest.

References

[1] B. Blobel, G. Stassinopoulos, P. Pharow, Model-based design and implementation of secure, interoperable EHR systems, AMIA Annu. Symp. Proc. 9 (2003) 6–100.

[2] J.L. Fernández-Alemán, I.M. Señor, P.A.O. Lozoya, A. Toval, Security and privacy in electronic health records: a systematic literature review, J. Biomed. Inform. 46 (3) (2013) 541–562.

[3] B. Kaplan, S. Litewka, Ethical challenges of telemedicine and telehealth, J. Cambridge Q. Healthcare Ethics 17 (4) (2008) 401–416.

[4] E.-H. Kluge, Health information, privacy, confidentiality and ethics, Int. J. Biomed. Comput. 35 (1) (1994) 23–27.

[5] E.-H. Kluge, Security and privacy of EHR systems—ethical, social and legal requirements, Stud. Health Technol. Inform. 96 (2003) 121–127.

[6] C.P. Waegemann, The five levels of electronic health records, MD Comput. 13 (May-June (3)) (1996) 199–203.

[7] S.W. Chen, D.L. Chiang, C.H. Liu, T.S. Chen, F. Lai, H. Wang, W. Wei, Confidentiality protection of digital health records in cloud computing, J. Med. Syst. 40 (May (5)) (2016) 124.

[8] A.S.Y. Cheung, R.H. Weber (Eds.), Privacy and Legal Issues in Cloud Computing, Edward Elgar, Cheltenham, UK, 2015.

[9] P.R. DeMuro, W.A.H. Gantt, HIPAA privacy standards raise complex implementation issues, Healthc. Financ. Manage. 55.1 (2001), 42–42.

[10] European Union Agency for Fundamental Rights. Handbook on European Data Protection Law. Luxembourg : Publications Office of the European Union (2014).

[11] J.L. Fernández-Alemán, I.C. Señor, P.Á. Lozoya, A. Toval, Security and privacy in electronic health records: a systematic literature review, J. Biomed. Inform. 46 (3) (2013 Jun) 541–562.

[12] Freshfields, Bruckhaus and Deringer. (2015) Privacy framework for the new world of e-health; accessed 2,1,2016 at http://www.freshfields.com/en/global/Digital/ehealth_privacy/.

[13] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, G. Müller, Aspects of privacy for electronic health records, Int. J. Med. Inform. 80 (February (2)) (2011) e26–31.

[14] L.B. Harman, C.A. Flite, K. Bond, Electronic health records: privacy, confidentiality, and security, Virtual Mentor 14 (September (9)) (2012) 712–719.
[15] B. Kaplan, How should health data Be used? Camb. Q. Healthc. Ethics 25 (2) (2016 Apr) 312–329.
[16] B. Kaplan, Selling health data: de-identification, privacy, and speech, Camb. Q. Healthc. Ethics 24 (July (3)) (2015) 256–271.
[17] L. Koontz, Health information privacy in a changing landscape, Generations 39 (1) (2015), 97-104(8).
[18] F. Li, X. Zou, P. Liu, J.Y. Chen, New threats to health data privacy, BMC Bioinf. 12 (Suppl. (12)) (2011) S7.
[19] OECD, Health Policy Studies Health Data Governance Privacy, Monitoring and Research. OECD Health Policy Studies, OECD Publishing, Paris, 2015.
[20] C. Petersen, P. Demuro, K.W. Goodman, B. Kaplan, v. Sorrell, IMS Health: issues and opportunities for informaticians, J. Am. Med. Inform. Assoc. 20 (1) (2013 Jan 1) 35–37.
[22] R.J. Rodriguez, P. Wilson, S.J. Schanz, The Regulation of Privacy and Data Protection in the Use of Electronic Health Information, PAHO, Washington, DC, 2001.
[23] S.J. Schanz, Compendium of Telemedicine Laws-Selected Statute Excerpts and Article Citations Relating to Telemedicine, Legamed, Raleigh, NC, 1999.
[24] US Department of Health and Human Services. Proposed Standards for Privacy of Individually Identifiable Health Information. (1999).
[25] K.T. Win, W. Susilo, Y. Mu, Personal health record systems and their security protection, Health Inf. Manage. 34 (1) (2005) 13–18.
[26] World Health Organization, Legal frameworks for eHealth: based on the findings of the second global survey on eHealth. (Global Observatory for eHealth Series, v. 5; accessed 2.6.2016 at http://apps.who.int/iris/bitstream/10665/44807/1/9789241503143_eng.pdf.
[27] K. Bennett, Legacy systems: coping with success, IEEE Software 12 (1) (1995) 19–23.
[28] J. Bisbal, D. Lawless, B. Wu, J. Grimson, Legacy information systems: issues and directions, IEEE Software 16 (1999) 103–111.
[29] Y.-G. Kim, Improving legacy systems maintainability, Information Systems Management 14 (1) (1997) 7–11.
[30] SiHIS Biennial Working Conference, International Medical Informatics Association, (Helsinki, September 30 – October 3, 1995).
[31] A.R. Chapman (Ed.), Health Care and Information Ethics: Protecting Fundamental Human Rights, Sheed and Ward, Kansas City, 1997.
[32] M.F. Collen, H. Shortliffe, The creation of a new discipline, in: Morris F. Collen, Marion J. Ball (Eds.), The History of Medical Informatics in the United States, Springer, 2015, pp. 75–120.
[33] D.E. Detmer, B.S. Munger, C.U. Lehmann, Medical informatics board certification: history, current status, and predicted impact on the medical informatics workforce, Applied Clinical Informatics 1 (1) (2010) 11–18.
[34] H. Rippen, A. Risk, E-Health code of ethics, J. Med. Internet Res. 2 (2) (2000) e9.
[35] International Medical Informatics Association. IMIA Code of Ethics for Health Information Professionals; available at http://www.imia-medinfo.org/new2/node/39.
[36] Sixty-Sixth World Health Assembly eHealth standardization and interoperability http://apps.who.int/gb/ebwha/pdf_files/WHA66/A66_R24-en.pdf.
[37] L. Kassell, Casebooks in early modern england: astrology medicine and written records, Bull. Hist. Med. 88 (2014) 595–625.
[38] E.L. Siegler, The evolving medical record, Ann. Intern. Med. 16 (10) (2010) 671–677 (153).
[39] E.-H. Kluge, The Ethics of Electronic Patient Records, Peter Lang, 2001.
[40] 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.
[41] Parliament of Europe, General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).
[42] OECD, Health Policy Studies Health Data Governance Privacy, Monitoring and Research. OECD Health Policy Studies, OECD Publishing, Paris, 2015.
[43] Court of Justice of the European Union. OJ C 165, 9.6.2012.
[44] E.-H. Kluge, Medical narratives and patient analogues: the ethical implications of electronic patient records, Meth. Inform. Med. 38 (1999) 1–7.
[45] 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.
[46] Nuremberg Trials State Parties/Signatories: Geneva Conventions of 12 August 1949. International Humanitarian Law. International Committee of the Red Cross.
[47] Kant, Critique of Pure Reason, A548/B576 p. 473.
[48] C. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (4) (1949) 656–715, http://dx.doi.org/10.1002/j.1538-7305.1949.tb00928.
[49] Personal communication, Najeeb Al-Shorbaji, Director, Knowledge Management and Health, WHO, Medinfo 2015, Sao Palolo, Brazil.
[50] F.H. Belgium: Roger France, C. Beguin, C. Mélot, P. Gillet, Board certified physicians in health informatics a European precedent for professional recognition, Yearb Med Inform. 11 (2010) 6–20.
[51] COACH Certification (CPHIMS-CA); available at http://www.coachorg.com/en/professionaldevelopment/Certification.asp.
[52] J.K. Iglehart, B. Robert, R.B. Baron, Ensuring physicians' competence — is maintenance of certification the answer? N. Engl. J. Med. 367 (2012) 2543–2549, http://dx.doi.org/10.1056/NEJMhpr1211043.
[53] United Nations Commission on International Trade Law; http://www.uncitral.org/uncitral/en/uncitral_texts.html.
[54] Court of Justice of the European Union; http://europa.eu/about-eu/institutions-bodies/court-justice/index_en.htm.
[55] United Nations General Assembly Case Law on UNCITRAL Texts (CLOUT); available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/V10/547/96/PDF/V1054796.pdf?OpenElement.