Ethical and Legal Considerations of Healthcare Informatics

Maria ALUAŞ

Iuliu Haţieganu University of Medicine and Pharmacy, Cluj-Napoca, Romania
Center for Bioethics, Babeş-Bolyai University, Cluj-Napoca, Romania
E-mail: maria.aluas@gmail.com

* Author to whom correspondence should be addressed; Tel.: 0040744880262.

Received: September 1, 2016/Accepted: November 22, 2016/ Published online: December 29, 2016

Abstract
Internet, cloud computing, social networks and mobile technology, all facilitate information transfer. Healthcare professionals, physicians and patients can use *informatic devices* in order to simplify their access to medical information, to streamline testing, and to understand clinical results. The use of computers and software facilitate doctor-patient interactions by optimizing communication and information flow. However, digital interfaces also increase the risks that information specialists use information without fully complying with ethical principles and laws in force. Our premise is that these information specialists should: 1) be informed of the rights, duties, and responsibilities linked to their profession and laws in force; 2) have guidelines and ethical tutoring on what they need to do in order to avoid or prevent conflict or misconduct; 3) have renewed specific training on how to interpret and translate legal frameworks into internal rules and standards of good practice. The purpose of this paper was: 1) to familiarize professionals who work in healthcare informatics with the ethical and legal issues related to their work; 2) to provide information about codes of ethics and legal regulations concerning this specific area; 3) to summarize some risks linked to wrong or inadequate use of patient information, such as medical, genetic, or personal data.

Keywords: Ethics; Informatics; Healthcare professionals; Informatics Codes of Ethics; Law regulations

"Technology is neither good nor bad, nor is it neutral"

– Kranzberg's First Law of Technology [1]

Introduction

At first glance, there seems to be little connection between health, informatics and ethics. Nonetheless, the concept of ethics, although present since Antiquity, seems to gain importance with the development of science and new technologies. In fact, professionals from different fields of activity, especially those who work in the healthcare system, need to respect principles, good practices and legal regulations in order to avoid damage and injuries to people.

In order to understand the present paper, some definitions must be clarified: first of all, the concept of ethics. **Ethics** is the art of behaving. Yet, reasons that determine our behavior are transformed by society [1]. As a result, ethics could hold different meanings depending on the countries, cultures, values, religions, and customs where it is defined. For the purpose of this paper, ethics means to behave in a proper way in accordance with your profession: to do what you say and

to say what you do.

Second, it is also important to define health informatics. While different definitions of health informatics exist, we considered the following to be the most appropriate in the present context. **Health informatics** is the scientific field dealing with "resources, devices, and formalized methods for optimizing the storage, retrieval and management of biomedical information for problem solving and decision making" [2]. The proposed definition implies that health informatics helps not only in resolving ethical conflicts, but also in preventing them. Although health informatics is known since the 1950s-1960s as a new area in the clinical setting, it has only recently been recognized as a distinct domain of health practice and research. Health information specialists need specific methods and procedures for using computers and software in order to enhance the way in which healthcare information is processed as well as to avoid and prevent conflicts. This brings us to a third definition: **Informatics Ethics**, which deals with ethical behaviors required from anyone handling data and information [3].

Therefore, the domain of Ethics in Healthcare Informatics is composed of two areas of investigation: **Healthcare Ethics** and **Informatics Ethics**. Ethics in Healthcare and Ethics in Information Technologies further intersect to form Healthcare Informatics Ethics (Figure 1).

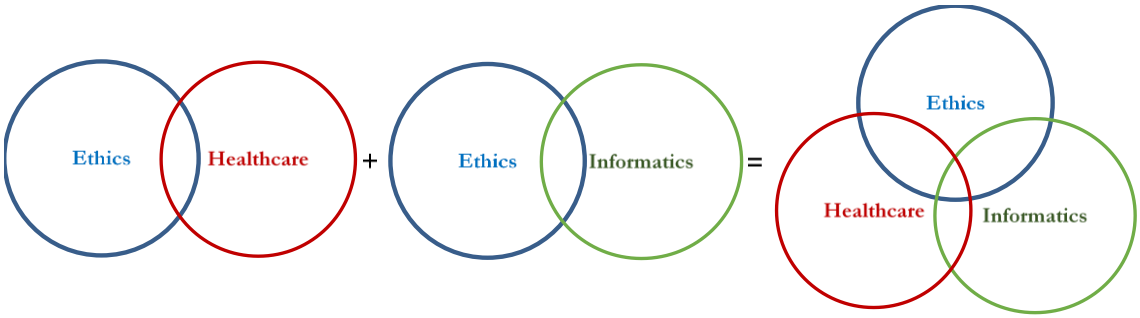

Figure 1. Healthcare Informatics Ethics is formed by Healthcare Ethics and Informatics Ethics

What is the need of ethics in healthcare informatics?

In clinical practice and research, healthcare professionals face issues regarding the proper legal and ethical use of software in appropriate disclosure of patient information, diseases, and risks. The transfer of medical data between healthcare organizations needs to be handled with appropriate security. Also, the medical database should be secured and professionals should be aware of good practices and guidelines in order to avoid and prevent conflicts or damages.

The aim of ethics in healthcare informatics is to raise awareness in professionals using healthcare informatics regarding the stakes and risks linked to information usage and ensure the enforcement of latest legal regulations and deontology codes. At the same time, proper knowledge of ethics in healthcare informatics should help professionals translate legal obligations into internal rules and guidelines.

Professionals who handle medical data should to be informed and trained on their duties. These duties, ethical principles, and law regulations are set up by some documents and frameworks, such as: legal regulations, deontology codes and guidelines.

Ethics Resources for Healthcare Informatics Professionals

Legal Regulations: International Conventions; EU Directives; national laws.

Legal regulations - such as conventions or national laws - are usually mandatory and sanctioned if trespassed.

Codes of Ethics are formal documents that list ethical principles and duties of professionals in a specific area. Organizations of professionals often adopt some codes in order to avoid or to

prevent misconduct and to protect human rights. For the purpose of this paper, we refer to the right to privacy and confidentiality of medical data.

Guidelines are defined, by Merriam Webster Dictionary [4], as rules or instructions that show or tell how something should be done. Guidelines or protocols are types of procedures that help healthcare professionals respect laws, principles and avoid misconduct.

Case studies help professionals better understand their situation by providing guidance and possible solutions for similar cases. These solutions are not mandatory and they cannot be applied as jurisprudence within the European civil law system (including Romania).

Ethics committees are consultative committees in a hospital or other institutions whose role is to analyze ethical dilemmas and advise and educate healthcare providers, patients and families regarding difficult ethical decisions [5].

In the following paragraphs we will present the main Codes of Ethics in Healthcare and Informatics and some legal regulations related to Healthcare and Informatics.

Principles and Codes of Ethics

As the Healthcare Informatics domain is composed by Healthcare and Informatics, there are several groups of principles, belonging to both areas.

First, it is necessary to consider the **principles of medical ethics**, set up, in the modern era by Beauchamps and Childress [6]. These principles are the following:

1. Autonomy: support others' informed, non-coerced freedom of thought and action; promote independence;
2. Beneficence: Responsibility to do good and promote others' welfare;
3. Non-maleficence: Obligation to do no harm or act in ways that have a high risk of harming others;
4. Justice: Act fairly or justly, especially balancing rights and interests of patients and others; afford all individuals the opportunity for equal access to the same high-quality diagnosis and treatment.

Second, the four principles of Information Ethics, introduced by Severson [7] in 1997, mention:

1. Respect for information property;
2. Respect for privacy;
3. Fair representation;
4. Non-maleficence or "doing no harm".

These principles are part of several Codes of Healthcare Informatics Ethics adopted by professional organizations, such as the World Health Organization (1997), the International Medical Informatics Association (2002), and the British Computer Society (2003). Furthermore, these principles are integrated by international, European, and national legal regulations, such as the Convention for the Protection of individuals with regard to automatic processing of personal data (1995). These codes present principles and general orientation for professionals who work in healthcare informatics.

Codes of ethics related to healthcare informatics

In 2002, the International Medical Informatics Association (IMIA) adopted the Code of Ethics for Health Information Professionals on data protection and health information. The code is available online in Croatian, Czech, Dutch, English, Japanese, Korean, Portuguese, Russian and Spanish [8].

The IMIA code of ethics serves several purposes:

1. It provides ethical guidance for the professionals themselves;
2. It provides a set of principles against which the conduct of professionals may be measured;
3. It provides the public with a clear statement of the ethical considerations that should shape the behavior of the professionals themselves.

This code also includes two sets of principles: fundamental ethical principles and general principles of informatics ethics. The fundamental ethical principles are: autonomy, equality and justice, beneficence, non-*malfeasance*, impossibility (meaning that duties and principles hold solely in applicable and 'possible' situations) and integrity. The general principles of informatics ethics are: information privacy and disposition, openness, security, access, legitimate infringement, least intrusive alternative, and accountability [8]. These principles relate to the notion, that all persons have a fundamental right to privacy.

The British Computer Society (BCS) adopted, in 2003, a Code of Ethics for Health Informatics Professionals (HIPs) [3]. This code is similar to the IMIA Code, which may be due to the shared contribution of one of its authors (Dr. Eike-Henner W. Kluge) [10].

Another code is the UK Council for Health Informatics Professions (UKCHIP) Code of Conduct [11], which is adapted from the BCS code [10]. "The UKCHIP Code of Conduct sets out standards of behavior required from health informatics professionals registered with the United Kingdom Council for Health Informatics Professions. It deals with all aspects of professional activity including registrants' duties to patients, the public, employers and colleagues." [11].

The UKCHIP Code of Conduct [11] requires that health informatics professionals:

- Work to high professional standards;
- Respect the rights and interests of others;
- Protect and act in the interests of patients and the public;
- Promote the standards and standing of the profession.

There are other ethics codes of health informatics ethics adopted by Canada's Health Informatics Association (COACH) [11] in 2004, by the American Health Information Management Association (AHIMA) [12] in 2006, and by the American Medical Informatics Association (AMIA) [13] in 2007.

These codes provide a simplified framework that allows professionals working in health informatics to avoid and prevent ethical and legal conflicts. A comprehensive table presented in Samuel et al. [9] and reproduced in Table 1, synthesizes the general ethical principles contained in the above codes. This table helps summarize and compare principles set up in these codes.

Table 1. General ethical principles in different codes (empty cells imply absence)

	Non-maleficence	Integrity	Equality & Justice	Beneficence	Autonomy	Impossibility
WHO	✓	✓	✓	✓	✓	✓
IMIA	✓	✓	✓	✓	✓	✓
UKCHIP	✓	✓	✓	✓	✓	✓
COACH	✓	✓	✓	✓		✓
AHIMA	✓	✓	✓	✓		✓
AMIA	✓	✓	✓	✓	✓	✓

Note: Reproduced from Samuel et al. [9] Table 1.

Legal regulations on healthcare informatics have not been adopted yet, but there are some other legal regulations related to the protection of medical data and professionals who deal with personal information.

International and European regulations on data protection

On the 28th of January 1995, the Council of Europe proposed a Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) [14]. Convention 108 is the first international tool related to personal data protection against any automatic processing abuse. The purpose of the Convention is "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (art. 1 about data protection).

The second regulation is the European Parliament Directive 95/46/CE [15], adopted in 1995. This directive deals with the protection of data and covers a wide range of issues from privacy to security. It is the main European norm on personal data protection. The principal objective of this directive is to harmonize protection rules of personal data in all countries of the European Union. Its principles have been synthetized by de Lusignan et al. [16], as follows:

- Personal data shall be processed fairly and lawfully;
- Personal data shall be obtained and processed for one or more specified and lawful proposes and not in any manner incompatible with those purposes;
- Personal data shall be adequate, relevant and not excessive in comparison to the purpose that it was collected for;
- Personal data shall be accurate and up-to-date where necessary;
- Personal data should not be kept longer than is deemed necessary;
- Personal data shall be processed in accordance with the rights of individuals, as set out in the act;
- Personal data shall have appropriate security measures in place;
- Personal data shall not be transferred outside of the European Economic Area (EEA) unless adequate protections exist for the rights and freedoms of data subjects.

Being elaborated in 1995, these principles do not cover realities of our times, such as the use of the Internet, social networks, or "cloud computing". Because of these new realities, the European Commission considered that it would be necessary to adapt and strengthen the existing legal framework in the European Union. On the 25th of January 2012, a regulatory proposal was submitted, which, once adopted, will replace the Directive 95/46/EC, with the advantage of being directly applicable to all EU Member States, as well as Norway, Iceland and Liechtenstein. The regulatory proposal emphasizes the rights of individuals on handling and processing of personal data and imposes new obligations regarding those responsibilities [17].

According to this legal framework, medical data are classified as personal data. These are sensitive data and, therefore, fall under specific protection measures. Medical data means "personal data concerning the state of health of the data subject are qualified as sensitive data", under Article 8 (1) of the Data Protection Directive and under Article 6 of Convention 108: "Medical data are subject to a stricter data-processing regime than non-sensitive data" [14].

Article 8 (3) of the Data Protection Directive allows for processing medical data where this is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services. Processing is permissible, however, only if performed by a healthcare professional subject to an obligation of professional secrecy, or by another person subject to an equivalent obligation.

Romanian Legal Framework on data protection

The Romanian laws in force regarding healthcare informatics are the following: the Criminal Code, art. 227, Law no. 95/2006 on healthcare reform and law no. 677/ 2001 on individuals protection regarding the processing of personal data.

In the Romanian Criminal Code, professional secrecy is regulated within article 227 which states that "disclosure without right of private data or information which may cause harm, disclosed by one who has access to personal data because of his/her profession or position and who has the obligation to maintain confidentiality, is punished by imprisonment from 3 months to 3 years, or by a fine" [18; translated loosely by MA]. The law doesn't define what secrecy means, but it is clear that it refers to the personal information which is known from the one who has the duty to preserve secrecy.

Law no. 95/2006 on healthcare reform [19] states in article 39 that "information on people's health is preserved by the territorial public health authorities, by the public health authorities of the ministries with own sanitary network, and by designated institutions and they can be used for

drawing up unnamed statistical reports, in order to assess the population's health". The use of these data for other purposes is authorized only under one of these four conditions:

a) There is a legal regulation in this respect;

b) There is consent from the person concerned;

c) The data are necessary to prevent an illnesses in an individual or a community;

d) Data are necessary for carrying out a criminal investigation.

Maintaining the confidentiality of medical information relating to individuals is mandatory for all employees whose activity is directly or indirectly related to this data, according to the same article 39 of this law.

Personal data, which also includes medical data, is regulated by the Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of such data [20]. Under the Law no. 677/2001, medical data are considered personal data, according to article 3 of this act. Article 4 states that data are processed taking into account the following principles: good faith; data are collected for specific and explicit purposes; data are adequate, relevant and not excessive in relation to the purpose; data are accurate and updated; data are deleted when no longer needed and kept strictly as necessary for the purpose.

Data are collected and processed under the following conditions:

- The person has consented expressly and unequivocally for that processing
- Professionals respect the principles set out in article 4.

Article 7 of this law refers to the existence of some special categories of data, such as: racial or ethnic origin; political, religious, philosophical or similar convictions; union membership; personal data concerning health conditions or sexual life. The processing of such data is prohibited, in principle, with some exceptions: 1) if the person concerned expressed explicit consent; 2) if the processing is carried out in legitimate activities by a foundation, association (...) and the data is processed with the condition that the person concerned is a member or participates in activities of this organization; 3) if the data are made public by the person concerned; 4) if the processing is necessary for preventive medicine, or to establishing medical diagnosis, providing care or medical treatments for the person concerned, only if the processing is done by a doctor. Health condition data processing can only be done by or under the supervision of medical staff (art. 9).

The National Supervisory Authority for Personal Data Processing, established by Law no. 102/2005, provided a new regulatory decision (Decision no. 200/2015) on the 14th of December 2015. According to this Decision, the processing of personal data is "any operation or set of operations which is performed upon personal data by automatic tools, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure to third parties by transmission, dissemination or otherwise, alignment or combination, blocking, erasure or destruction".

Final Remarks

In this paper, we tried to familiarize professionals who work in healthcare informatics with the context of this kind of work: definitions, delimitations of concepts, ethical and legal frameworks regarding the exercise of this profession. We also examined the main codes of ethics adopted by international professional organizations and the laws in force regarding the protection of personal data, privacy and confidentiality. We summarized some risks linked to wrong or inadequate usage of information about patients, such as medical, personal data. This paper presents an overview of the main issues in healthcare informatics ethics and some reasons for which professionals in healthcare informatics should be informed and be aware of the importance and relevance of such issues and codes to avoid and prevent conflicts and misconduct.

These topics should continue to be deeply explored and debated by all involved.

Conflict of Interest

The author declares that she has no conflict of interest.

References

1. Salmon R. 21 Defis pour le XXIe siècle. Paris: Ed. Economica; 2002, p. 53.
2. Shortlife I. What is Medical Informatics. Lecture. Standford University 1995, cited by R. E. Hoyt, E. V. Bernstam, Overview of Health Informatics. In Hoyt R.E., Bailey N., Yoshihashi A. Health Informatics: Practical Guide for Healthcare and Information Technology Professionals, 5th edition, [Raleigh, N.C.]: Lulu.com [online] 2012, [cited 2016 August 20]. Available from: URL:https://books.google.ro/books/about/Health_Informatics_Practical_Guide_for_H.html?id=49eSAwAAQBAJ&redir_esc=y/.
3. Health Informatics Committee, British Computer Society. A handbook of Ethics for Health Informatics Professionals, 2003. [cited 2016 August 20]. Available from: http://www.bcs.org/upload/pdf/handbookethics.pdf.
4. Merriam Webster Dictionary. Guideline's definition. [cited 2016 August 21]. Available from: http://www.merriam-webster.com/dictionary/guidelines.
5. U.S. Congress, Office of Technology Assessment, Life-Sustaining Technologies and the Elderly, OTA-BA-306. Washington, DC: U.S. Government Printing Office, July 1987. [cited 2016 August 22]. Available from: http://govinfo.library.unt.edu/ota/Ota_3/DATA/1987/8714.PDF.
6. Beauchamp TL, Childress JF. Principles of biomedical ethics, New York: Oxford University Press: 1979.
7. Severson R. The Principles of Information Ethics. New York: M. E. Sharp, 1997.
8. International Medical Informatics Association (IMIA). Code of Ethics for Health Information Professionals. 2002 [cited 2016 Aug 16] Available from: URL: http://imia-medinfo.org/new2/node/39
9. Samuel HW, Zaïane OR, Sobsey D. Towards a Definition of Health Informatics Ethics. IHI'10, November 11-12, 2010, Arlington, Virginia, USA. [cited 2016 August 22]; Available from: URL: https://webdocs.cs.ualberta.ca/~zaiane/postscript/ACMIHI2010.pdf.
10. UK Council for Health Informatics Professions. UKCHIP Code of Conduct. Retrieved March 4, 2010 [cited 2016 August 20]. Available from: http: /www.ukchip.org/?q=page/UKCHIP-Code-Conduct.
11. Samuel HW, Zaïane OR. A Repository of Codes of Ethics and Technical Standards in Health Informatics. Online J Public Health Inform. 2014; 6(2): e189. [cited 2016 August 22]; Available from: URL: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4235322/
12. American Health Information Management Association (AHIMA). Code of Ethics. 2006. Revised & adopted by AHIMA House of Delegates – (October 2, 2011). [cited 2016 August 22]; Available from: URL: http://bok.ahima.org/doc?oid=105098#.V8U1nL55LRq.
13. American Medical Informatics Association (AMIA). A Code of Professional Ethical Conduct. 2007. [cited 2016 August 22]; Available from: URL: https://www.amia.org/about-amia/ethics
14. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. European Treaty Series No. 108. Strassbourg; 28.01.1981. [cited 2016 August 22]; Available from: URL: http: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37.
15. European Parliament, European Council. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 24 October 1995. [cited 2016 August 22]; Available from: URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.
16. De Lusignan S, Chan T, Theaom A, Dhoul N. The role of policy and professionalism in the

protection of processed clinical data: A literature review. Int. J. Med. Inf. 2007; 76:261-8. [cited 2016 August 26]; Available from: URL: http://www.ncbi.nlm.nih.gov/pubmed/16406791. Cited by Masters K. in Health Informatics: Practical Guide for Healthcare and Information Technology Professionals, 5th edition, [Raleigh, N.C.]: Lulu.com [online] 2012. Chapter 10, Health Informatics Ethics; p. 195-215.

17. Aluaș M. The protection of genetic data resulting from internet tests. In: Vasiu I, Streteanu F. (Eds.) Preventing and combating cybercrime. Cluj-Napoca: Accent; 2016, p. 212-219.
18. Law no. 286/2009 on New Criminal Code (Legea nr. 286/2009 privind noul Cod Penal). Monitorul Oficial nr. 510 din 24 iulie 2009). In force from 1st February 2014 (*journal*); Bogdan S, Serban D.A., Zlati G. Noul Cod penal. Partea speciala. Analize, explicatii, comentarii. Bucuresti: Universul Juridic; 2014.
19. Law no. 95/2006 on health reform (Legea nr. 95/2006 privind reforma în domeniul sănătăţii). Monitorul Oficial nr. 372 din 28 aprilie 2006.
20. European Union Agency for Fundamental Rights, Council of Europe. Handbook on European data protection law. Luxembourg: Publications Office of the European Union, 2014. 173-74 [cited 2016 August 26]; Available from: URL: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.