Towards a Definition of Health Informatics Ethics

Hamman W. Samuel
Department of Computing Science
University of Alberta
Edmonton, Alberta, Canada
hwsamuel@cs.ualberta.ca

Osmar R. Zaïane
Department of Computing Science
University of Alberta
Edmonton, Alberta, Canada
zaiane@cs.ualberta.ca

Dick Sobsey
John Dossetor Health Ethics Centre
University of Alberta
Edmonton, Alberta, Canada
dsobsey@ualberta.ca

ABSTRACT

Information technology is a prominent tool in healthcare management. However, healthcare systems often fall short of addressing concerns about privacy, confidentiality and safety of information. Even though there is existing literature on ethical issues in medicine, as well as ethics in computing, information technology in medicine leads to new ethical issues that are not covered by medical or computing ethics. We define the term 'health informatics ethics' to encompass ethical issues resulting from the use of technology in managing healthcare information. We also investigate the application of our proposed definition to not only resolving ethical conflicts, but also preventing conflicts.

Categories and Subject Descriptors

K.7.4 [**The Computing Profession**]: Professional ethics—*codes of ethics*; K.4.1 [**Computers and Society**]: Public Policy Issues—*ethics*

General Terms

Theory

Keywords

ethics, health informatics

1. INTRODUCTION

There is extensive literature on the subject of ethical conduct and principles in medicine. Similarly, there are existing bodies of knowledge on ethics in computing and information technology. It can be argued that these two bodies of literature cover ethical issues in health informatics. However, we point out that information technology and medicine together lead to new issues in ethics.

Medical devices and healthcare information systems rely on software, which has the tendency to fail. Because these devices and systems are safety-critical to people, the issue of ethics comes into play. The Therac-25 medical accelerator is one of the many examples of software bugs causing loss of lives. Because of a bug in the underlying operating system of the Therac-25 X-ray device, five patients died due to overexposure, while many others were seriously injured[1].

Furthermore, the use of information systems in healthcare leads to more complicated scenarios about safety and confidentiality. For example, the Physician's Alert software system allows doctors to identify if a patient has sued a doctor in the past. Doctors may use this kind of information to refuse patient care, even though it goes against the credo of providing patient care[1].

Ethics issues in health informatics require more than just interdisciplinary cooperation in the fields of ethics, medicine, and computing. These issues are markedly important due to the vulnerability of people needing care and potential risks of using information technology to provide this care. In this study, we examine and synthesize codes of ethics from leading computer and health informatics bodies into a concise view of the notion of health informatics ethics. We examine codes from the British Computer Society (BCS), International Medical Informatics Association (IMIA), Association for Computing Machinery (ACM), IEEE, and guidelines from the U.S. Food and Drug Administration (FDA), among others. We also investigate how existing body of knowledge addresses ethics in health informatics with the view of resolving, as well as preventing ethical conflicts.

2. RESOLVING ETHICAL CONFLICTS

Ethics deals with decisions about right versus wrong, good versus bad. These normative and moral questions involve people and how they affect each other[18]. An ethical conflict is opposition between moral ideas or interests. In the case of the Physician's Alert system, doctors' interests in not getting sued are conflicting with their duty towards the patient. In another case, the HIV Treatment Data Project aims to create a website that contains patient testimonials on antiretroviral drugs. On one hand, the privacy of the patients needs to be preserved, but doing so would make the testimonials ineffective in reaching out to help other HIV patients. More importantly, the imperative to do good to others can be seen in conflict with the patients' need for privacy[1].

What is to be done in the face of these conflicts? In our two examples, should the doctors be allowed to deny care? Or should the anonymity of the HIV patients be preserved or not?

IHI'10, November 11–12, 2010, Arlington, Virginia, USA.

2.1 Ethics Resources

To help resolve such issues and answer the hard questions, there are various ethical resources available: codes of ethics, case studies, ethics committees and personnel, and informal discussions[17]. These resources help in determining which course of action to take.

2.1.1 Codes of ethics

Ethics codes are formal documents that list ethical principles and duties. Members of the profession or organization are required to adhere to the principles of these codes to guide their ethical conduct. In addition, these codes serve to correct any wrong notions about ethical principles.

2.1.2 Case studies

There are often available reference to similar ethical conflicts and situations in the past that may have been resolved in a certain manner. These cases can be applied as jurisprudence.

2.1.3 Ethics committees and personnel

Organizations can have committees and trained staff to discuss and resolve ethics issues. These may include ethics boards or ethics professionals that are contacted for consultation when ethical conflicts occur.

2.1.4 Informal discussions

Chats with friends or colleagues can lead to informal advise about how an ethical conflict can be resolved.

In the context of this study, we concentrate on the use of codes of ethics. We do this because ethics codes provide a more formal framework.

2.2 Codes of Ethics in Health Informatics

We now present the codes of ethics used in this study, from the following national and international bodies.

- World Health Organization (WHO)
- International Medical Informatics Association (IMIA)
- British Computer Society (BCS)
- Canada's Health Informatics Association (COACH)
- American Health Information Management Association (AHIMA)
- American Medical Informatics Association (AMIA)

In making our selection, our goal was to cover international bodies as well as major regional bodies. These codes provide a simplified framework that allows ethical conflicts in health informatics to be resolved. Figure 1 shows the timeline of when these codes were published, as well as how the codes are related in terms of referencing one another[1].

2.2.1 International Codes

The International Medical Informatics Association (IMIA) Code of Ethics for Health Informatics Professionals is very comprehensive and covers duties of health informatics professionals from three perspectives: fundamental ethics principles, informatics ethics principles, and rules of ethical conduct in health informatics. We also use the World Health Organization (WHO) eHealth Code of Ethics, which is specifically for health-related websites[21].

[1]The UKCHIP code is not featured because the publication date is not explicitly stated.

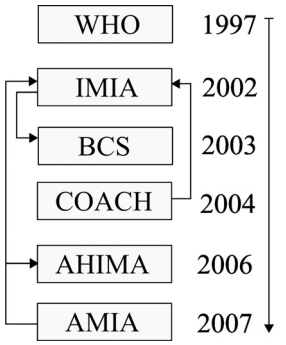

Figure 1: Timeline and Connections of Health Informatics Codes

2.2.2 British Codes

The Computer Society (BCS) Code of Ethics for Health Informatics Professionals and IMIA codes have shared authorship by Dr. Eike-Henner W. Kluge, and the BCS code contains the same material as the IMIA code. The BCS code is acknowledged by the IMIA as an accompanying handbook[4]. Similarly, the UK Council for Health Informatics Professions (UKCHIP) Code of Conduct is adapted from the BCS code[11].

2.2.3 Canadian Code

The COACH High-level Ethical Principles is published by Canada's Health Informatics Association and an abridged version containing ten aspirational high-level principles is available to the public. The full version of the code is available for members only[12].

2.2.4 American Codes

The American Health Information Management Association (AHIMA) Code of Ethics contains eleven ethical obligations expected of AHIMA members[3]. Another US code, the American Medical Informatics Association (AMIA) Code of Ethics is a fairly recent publication. The AMIA code references the AHIMA and IMIA codes and focuses more on duties of health informatics professionals expected towards key stakeholders in healthcare[15].

3. HEALTH INFORMATICS ETHICS

In the previous case of HIV treatment data, one resolution can be that we apply the BCS code's section on 'information privacy and disposition'. We observe that the right of the patient to privacy out-weighs any benefits that can be achieved from releasing their testimonials[8]. We now present a definition of health informatics ethics in the premise of codes of ethics.

Health informatics is about using computers to enhance the way health information is processed[22]. There are 3 aspects of health informatics that can be identified: healthcare, information, software[13, 10].

Healthcare

Health informatics is in the context of healthcare. Information systems are developed to facilitate dispensation of

healthcare or the auxiliary activities involved in healthcare. For instance, information systems for managing hospital infrastructure such as bed allocation are meant to enhance the care given to patients.

Information

Health informatics deals with efficiently processing information. A myriad of information about patients needs to be stored for future reference, and retrieved when needed. This includes Electronic Medical Records (EMRs), Patient Medical Records (PMRs), and many others. Transfer of information between healthcare organizations needs to be handled with proper security. In addition, information about medical personnel and staff needs to be stored and retrieved as well.

Software

Information is processed, stored, and retrieved effectively by using software. Enterprise-wide software systems are needed to manage clinics and hospitals, as well as information needed by larger healthcare providers.

Given these components in health informatics, we can define health informatics ethics in terms of ethical dimension for each component, as illustrated in Figure 2. Consequently, health informatics professionals need to adhere to these 3 ethical dimensions of their profession[8, 4].

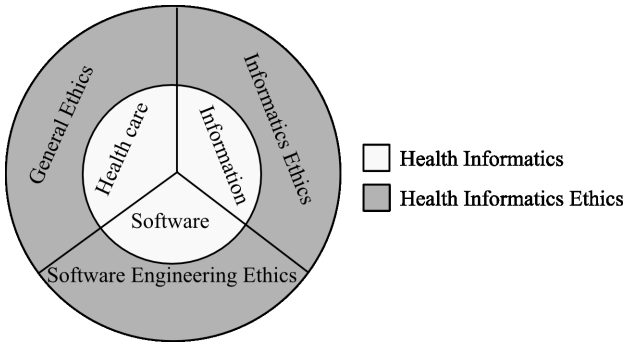

Figure 2: Health informatics ethics

3.1 General Ethics

The first dimension to health informatics ethics is general ethics, in cognisance with healthcare. All our social interactions dealing with norms and values are guided by ethics. Whenever and however we interact with people, we ought to be guided by these general principles. The BCS/IMIA code defines general ethics using six major principles, which need to be adhered to by every member of society[8, 4].

3.1.1 Non-malfeasance

We have a duty to prevent harm to others without undue harm to ourselves. All members of society are expected to value life and protect it, by not engaging in activities that cause harm.

3.1.2 Integrity

We have a duty to fulfill our obligations to the best of our abilities. Every member of society is expected to be honest and diligent.

3.1.3 Equality and justice

We have the right to be treated equally. Members of society ought to treat their fellow members equally, without discrimination.

3.1.4 Beneficence

We have a duty to advance the good of others. A member of society does not seek just his or her own good, but the general good and advancement of the society as a whole.

3.1.5 Autonomy

We have the right to self-determination. Members of society ought to be given independence in making decisions and judgements.

3.1.6 Impossibility

All our duties are subject to our ability to do them.

As an example, in-line with the principle of impossibility, a surgeon cannot be 100% sure about the success of an operation. However, because of the principle of integrity, the surgeon performs the operation to the best of his or her agreement. In Table 1, we investigate the codes for general principles using the BCS code as anchor. A notable observation is that the COACH and AHIMA codes do not address the issue of autonomy, and have no specifications for facilitating patients or clients to make self-decisions.

3.2 Informatics Ethics

Informatics ethics is the second dimension to health informatics ethics. Informatics ethics deals with ethical behavior required of anyone handling data and information[8, 4]. In this information age, ethical conduct is required in our handling of information as well. For instance, in March 1999, the sexual and medical histories of several people were found by a reporter on the Internet using a public-use search engine. Even though this was not a malicious and sophisticated attack to invade privacy, the handling of this sensitive information was ethically questionable[1]. The following seven principles are stated in the BCS/IMIA code to define informatics ethics.

3.2.1 Privacy

Everyone has the right to privacy of their own information. Every person has the right to decide how much information they wish to disclose about themselves, and what information they wish to withhold. Furthermore, individuals have the right to control what information is collected, how it is stored, and used.

3.2.2 Openness

Data collection about any person must be done transparently. This implies that the person about whom the data is being collected needs to be informed of the intent for collecting data and what the data will be used for.

3.2.3 Security

Data collected must be protected. Once data is collected, it must be safeguarded against unauthorized access by other parties. In addition, the data needs to be protected against manipulation, both malicious and unintentional.

	Non-malfeasance	Integrity	Equality & justice	Beneficence	Autonomy	Impossibility
WHO	⊕	⊕	⊕	⊕	⊕	⊕
IMIA	⊕	⊕	⊕	⊕	⊕	⊕
UKCHIP	⊕	⊕	⊕	⊕	⊕	⊕
COACH	⊕	⊕	⊕	⊕		⊕
AHIMA	⊕	⊕	⊕	⊕		⊕
AMIA	⊕	⊕	⊕	⊕	⊕	⊕

Table 1: General Ethical Principles in the Codes, ⊕ implies existence, empty cell implies absence

3.2.4 Access

Everyone has the right to access and correct their own data. An individual's data should not be kept in isolation and allowed to become outdated.

3.2.5 Legitimate infringement

Access is subject to legitimate data needs of a free society. The individual's right to privacy and access may be infringed upon if doing so would be for the larger good of society.

3.2.6 Least intrusive alternatives

Any legitimate infringement must be done with minimum interference to the rights of the person affected. Legitimate infringement of an individual's data does not give free reign.

3.2.7 Accountability

Legitimate infringement must be reported to the person affected in due time. This implies that eventually the affected individual should be notified of the nature and reason for infringement.

In Table 2, we present what informatics principles are covered in the various codes, again using the BCS/IMIA code as anchor. We observe that the WHO code does not directly address security, but makes vague reference to it in terms of privacy. Also, the principles in the WHO code are opposing the BCS principles of legitimate infringement and least intrusive alternatives, because the WHO code requires prior, explicit, and unconditional approval from the person whose information is to be accessed. The UKCHIP code does not address these 2 principles either. In addition, the UKCHIP code leaves out openness and accountability. The COACH code is also missing various principles, but this can be expected since it presents high-level principles. Similarly, the AHIMA and AMIA codes have a few missing principles. The indication is that most of the other codes are more focused on general ethics.

3.3 Software Engineering Ethics

Our third dimension to health informatics ethics is software engineering ethics, which can be defined in terms of activities carried out by software developers that have the potential of affecting end-users[14]. For example, it was reported in the news that the Illinois medical center's files were hacked into by a computer engineer[1]. Even though hacking is a glaring example, software engineers need to be ethically responsible, especially when sensitive data such as health information is involved. A joint task force by IEEE and CS-ACM drafted a code of ethics for software engineers that contains the following 8 principles[6].

3.3.1 Public

Activities are done with the best interest of the society in mind. Developers should be aware of social impacts of software systems; in the process of developing these systems as well as eventual usage of such systems. This includes disclosing any dangers or known defects in software.

3.3.2 Client and employer

Activities are done in the best interests of clients and employers. Developers are obliged to have the interests of their clients in mind, while balancing their duties to the public. This also encompasses being forthright about personal limitations and qualifications, as well as maintaining privacy and confidentiality about information of the client.

3.3.3 Product

Software products should meet expected professional standards. Developers should strive to build products that are not sub-standard. Developers should ensure that the product is thoroughly tested and debugged, and unsolved problems are documented.

3.3.4 Judgment

Integrity and independence is kept in making decisions about software development. Developers should avoid situations in which they or their clients have conflicts of interest, either internally or with other parties.

3.3.5 Management

Managers and leaders should subscribe to ethical approaches in software development. Realistic and effective costs, schedules, and procedures should be promoted. In addition, developers should be aware of their client or employer's policies.

3.3.6 Profession

The reputation of the software engineering profession should be advanced. Developers should promote and facilitate education of software engineering and point out anyone who violates the profession's standards and codes.

3.3.7 Colleagues

Colleagues are to be supported and treated fairly. This includes support in development, as well as in understanding of the profession's codes. Developers are to fully credit their colleagues for their work, including intellectual contributions and code re-use.

3.3.8 Self

Re-training and improvement is to be pursued by the software developer. In addition, developers should not let prejudices lead to unfair treatment of others. Furthermore, developers should not encourage others, directly or indirectly, to perform actions that violate the profession's code.

	Privacy	Openness	Security	Access	Legitimate infringement	Least intrusive alternative	Accountability
WHO	⊕	⊕		⊕			⊕
IMIA	⊕	⊕	⊕	⊕	⊕	⊕	⊕
UKCHIP	⊕		⊕	⊕			
COACH	⊕		⊕				
AHIMA	⊕		⊕				⊕
AMIA	⊕	⊕	⊕	⊕	⊕	⊕	⊕

Table 2: Informatics Ethical Principles in the Codes, ⊕ implies existence, empty cell implies absence

3.4 Stakeholders in Health Informatics Ethics

The definition of health informatics ethics in terms of general, informatics, and software engineering ethics encompasses principles promoted by various codes of ethics. However, it is equally important to identify the stakeholders involved in the health informatics setting because ethical conflicts arise as a result of interactions between these stakeholders. From the BCS/IMIA code, six types of professional relationships are listed that the health informatics professional is involved with[8, 4].

3.4.1 Patient

This refers to anyone who makes use of healthcare services, which generate electronic records for that individual, i.e. electronic medical records (EMRs), patient medical records (PMRs), etc.

3.4.2 Healthcare professionals

This includes doctors, nurses, and other medical staff that care for patients. They are different from health informatics professionals, i.e. those who work with health informatics systems.

3.4.3 Institutions and employers

Institutions/employers refers to who the health informatics professional is working for. This can be software agencies or healthcare facilities.

3.4.4 Society

This is a generalization of everyone else to whom the health informatics professional has duties, excluding patients, healthcare professionals, and employers.

3.4.5 Self

The health informatics professional has personal ethical duties, to which they should adhere.

3.4.6 Profession

Health informatics professionals relate with colleagues, and represent the health informatics profession in general

Table 3 illustrates a comparison of stakeholders in the BCS/ IMIA and the ACM/ IEEE codes. From a health informatics professional's point of view, a client and healthcare professional is distinct from an employer. However, from a software engineer's perspective, healthcare professionals and patients can be regarded as clients. This is because doctors, staff, and even patients eventually become end-users to the health software products. Also, the BCS/IMIA code covers relationships with colleagues under the profession, whereas the ACM/IEEE code specifically addresses this. Nevertheless, potential relationships leading to ethical conflicts are all covered in both codes.

4. BEYOND RESOLUTION: PREVENTING ETHICAL CONFLICTS

In the previous sections, we defined health informatics ethics in terms of *principles* in relevant codes of ethics. This definition allows the resolution of ethical conflicts, because the relevant stakeholders can be held responsible for not performing their duties stated in the codes. However, health informatics ethics can also be defined as a set of *activities* by health informatics professionals. Ethical conflicts may be preventable even before they happen if these activities are followed during development of health informatics systems.

As an example, a small hospital decided to implement a computer-based pharmacy system due to rapid growth and need for more efficiency. However, its user interface was modeled on a warehouse inventory system. Even though the functions specified were met, this led to excessive time for data entry and errors by the medical staff. This had not been anticipated by the developers. Whereas the developers had fulfilled user specifications, users would now blame errors in entry on the software, leading to a conflict of whom to blame[17].

Prevention of this ethical conflict could have been possible if some technical guidelines had been followed. However, the codes of ethics are not meant to be technical guides. In addition, following technical guidelines alone does not ensure that ethical conflicts will not ensue. The Food and Drug Administration (FDA) does indeed provide a document that aims to minimize software errors and failures through life cycle and risk management. In this section, we present these FDA guidelines as a resource for preventing ethical conflicts.

The FDA document titled 'General Principles of Software Validation' was created to reduce software defects and recalls resulting from these defects. The document applies to medical software or devices containing software. Its goals include reducing risk to patients and users, and also reduce liability to manufacturers of medical software. The FDA document achieves this through providing explicit guidelines on how to validate software during the stages of software development. Software validation is defined by the FDA as 'confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consistently fulfilled'[19]

4.1 Software Development Life-cycle

Development of health informatics systems involves going through the software development life-cycle (SDLC). In general, the software development life-cycle consists of all the stages during the development of software. We propose that by infusing ethical concerns in the SDLC, ethical conflicts can be reduced in the final product. This is achieved by adherence to the FDA guidelines for the SDLC. There

		BCS/IMIA					
		Society	Institutions & employers	Profession	Healthcare professionals	Patient	Self
ACM/IEEE	Public	⊕					
	Client & employers		⊕		⊕	⊕	
	Profession			⊕			
	Colleagues			⊕			
	Self						⊕

Table 3: Stakeholders in Health Informatics Ethics

are various SDLC models based on different software engineering paradigms. However, the FDA document does not conform to any one model, but provides the following generic SDLC model[19].

4.1.1 Quality planning

Tasks and procedures for reporting anomalies in software and resolving them are identified. In addition, potential risks, assumptions, and quality factors need are outlined. Furthermore, responsibilities for reviews and approvals assigned to specific personnel should be documented, as well as any other responsibilities.

4.1.2 Requirements

Information about the device or software and its intended use is identified, including proper documentation of the software or device functions. Safety precautions and possible hazards should also be documented so that countermeasures can be planned.

4.1.3 Design

Requirements are translated into a logical and physical representation of the software through design activities. In addition, the possibilities of usage errors need to be incorporated into the design by including appropriate testing measures. Both high-level and low-level specifications may be needed, since a large group of developers with varying technical know-how typically work together.

4.1.4 Coding

Software is usually constructed by either coding or by assembling coded components. This is the culmination of the design into a medical device or software product. Depending on the coding guidelines being opted for by the developers, there needs to be verification of this compliance, for example, commenting or documentation styles, and so forth.

4.1.5 Testing by Software Developer

This involves running the software with pre-defined inputs and known outputs in order to compare its accuracy. Reporting and documentation methods for defects should be clearly identified. Even though testing cannot be exhaustive, all efforts need to be taken for thorough testing of the code.

4.1.6 User site testing

This involves testing on-site with the user with realistic data. Apart from testing the correctness of the software or device with real data, tests are needed to determine if the user correctly understands usage of the interface.

4.1.7 Maintenance

This covers both installation and deployment of the software, as well as future changes to software that will require re-validation.

Software validation involves providing documentation of plans and procedures for risk management during each of these stages of the SDLC. In addition, the FDA document provides a template of tasks and activities for each stage of the SDLC, depending on the level of risk associated with the device or software. Needless to say, items that are more risky go through more activities before approval. These tasks are meant to support claims that software is validated and contains no obvious errors. The details of each task can be found in the FDA document[19]. Table 4 presents a summary of the tasks.

Eventually, the plans, procedures, and documented activities need to be evaluated and approved by the FDA. The FDA recommends independent evaluation and self-evaluation before final submission. In independent evaluation, the documentation for submission is evaluated by third parties[19].

4.2 Levels of Concern

In the SDLC, the specific tasks recommended by the FDA for validation depend on the level of concern, which is an estimate of the danger a device or software poses to a patient or operation. There are 3 levels of concern detailed in the FDA supplementary document titled 'Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices'. The level of concern for a given software is determined by answering a set of key questions contained within the FDA supplementary document[20].

Major

Possibility of death or serious injury to patient or operator, which may be as a result of a possible error or bug, or because of delays in information.

Moderate

Possibility of minor, non-fatal injury to patient or operator.

Minor

Almost unlikely to cause any injury to patient or operator.

4.3 Health Informatics Ethics as an Activity

In the preceding sections, we presented health informatics ethics as a set of activities that are incorporated into the SDLC. In our definition, health informatics ethics as an activity involves software validation, in accordance with the FDA guidelines. These guidelines are distinct from the health informatics ethics codes, as the former is more technical. This is also true for the ACM/IEEE code which provide guidelines on 'what' is ethical, whereas the FDA document

Quality planning	Requirements	Design	Coding	Testing by Software Developer	User site testing	Maintenance
Risk management plan	Preliminary risk analysis	Updated software risk analysis	Traceability analyses	Test planning	Acceptance test execution	Software validation plan revision
Configuration management plan	Traceability analysis	Traceability analysis	Source code and source code documentation evaluation	Structural test case identification	Test results evaluation	Anomaly evaluation
Software quality assurance plan	Description of user characteristics	Software design evaluation	Source code interface analysis	Functional test case identification	Error evaluation	Problem identification and resolution tracking
Problem reporting and resolution procedures	Listing of characteristics and limitations of primary and secondary memory	Design communication link analysis	Test procedure and test case generation	Traceability analysis	Final test report	Proposed change assessment
Other support activities	Software requirements evaluation	Module test plan generation		Unit test execution		Task iteration
	Software user interface requirements analysis	Integration test plan generation		Integration test execution		Documentation updating
	System test plan generation	Test design generation		Functional test execution		
	Acceptance test plan generation			System test execution		
	Ambiguity review or analysis			Acceptance test execution		
				Test results evaluation		
				Error evaluation		
				Final test report		

Table 4: Typical Tasks and Activities

defines 'how' to make it ethical. The emphasis on validation in the FDA document facilitates the eventual production of software that is sensitive to ethical issues arising from software faults. In other words, following the FDA software validation guidelines leads to the development of software that mitigates harm and upholds the ethical principle of 'non-malfeasance'. This software, which we refer to as 'ethical software', can prevent ethical conflicts. However, the FDA document only serves to reduce errors in software, consequently making software safer and not causing harm to others. Other principles such as privacy are not addressed as a result of the activity of software validation.

5. CONCLUSION AND FUTURE WORK

In this study, we investigate ethical conflicts in health informatics. We examine codes of ethics from the BCS/IMIA, ACM/IEEE, and others. We also investigate how the FDA guidelines is applied to building of health informatics software. As a result, we define health informatics ethics in terms of ethical principles and activities. Our contributions include comparative analysis of various health informatics ethics codes, and a synthesis of ethics codes and software validation guidelines into a comprehensive definition of health informatics ethics. However, the definition of health informatics as an activity is still narrow, covering only safety. In the future , the definition of health informatics ethics as an activity will be broadened to incorporate other guidelines that specifically address other ethical principles such as privacy, anonymity, security, and accountability, to mention a few.

6. REFERENCES

[1] J. G. Anderson and K. W. Goodman. *Ethics and Information Technology: A Case-Based Approach to a Health Care System in Transition*. Springer New York, 2002.

[2] R. E. Anderson, D. G. Johnson, D. Gotterbarn, and J. Perolle. Using the New ACM Code of Ethics in Decision Making. *Communications of the ACM*, 36(2):98–107, 1993.

[3] A. H. I. M. Association. American Health Information Management Association Code of Ethics. `http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_024277.hcsp?dDocName=bok1_024277`. Retrieved March 30, 2010.

[4] I. M. I. Association. The IMIA Code of Ethics for Health Information Professionals. `http://www.imia.org/pubdocs/Ethics_Eng.pdf`, 2002. Retrieved February 11, 2010.

[5] Association for Computing Machinery. ACM Code of Ethics and Professional Conduct. `http://www.acm.org/about/code-of-ethics`, 1992. Retrieved April 8, 2010.

[6] Association for Computing Machinery, Institute for Electrical and Electronics Engineers. Software Engineering Code of Ethics and Professional Practice. http://www.acm.org/about/se-code, 1999. Retrieved March 5, 2009.

[7] L. Colero. A Framework For Universal Principles of Ethics. http://www.ethics.ubc.ca/papers/invited/colero.html. Retrieved March 4, 2009.

[8] B. C. S. H. I. Committee. A Handbook of Ethics for Health Informatics Professionals. http://www.bcs.org/upload/pdf/handbookethics.pdf, 2003. Retrieved January 27, 2010.

[9] P. Duquenoy, C. George, and K. Kimppa. *Ethical, Legal, and Social Issues in Medical Informatics*. IGI Global, 2008.

[10] U. C. for Health Informatics Professionals. Professionalism in Health Informatics. http://www.ukchip.org/?q=page/Professionalism-Health-Informatics. Retrieved April 22, 2010.

[11] U. C. for Health Informatics Professionals. UKCHIP Code of Conduct. http://www.ukchip.org/?q=page/UKCHIP-Code-Conduct. Retrieved March 4, 2010.

[12] N. Gabor, J. MacGregor, and M. Murray. Ethical Principles: A Step Toward 'Professionalism' for COACH. *Healthcare Information Management and Communications Canada*, pages 32–34, 2006.

[13] K. W. Goodman. *Ethics, Computing, and Medicine: Informatics and the Transformation of Health Care*. Cambridge University Press, 1998.

[14] D. Gotterbarn. Software Engineering Ethics. In *Encyclopedia of Software Engineering*, volume 2, 2001.

[15] J. F. Hurdle, S. Adams, J. Brokel, B. Chang, P. J. Embi, C. Petersen, E. Terrazas, and P. Winkelstein. A Code of Professional Ethical Conduct for the American Medical Informatics Association: An AMIA Board of Directors Approved White Paper. *Journal of the American Medical Informatics Association*, 14(4):391–393, 2007.

[16] G. Marckmann and K. W. Goodman. Introduction: Ethics of Information Technology in Health Care. *International Review of Information Ethics (IRIE)*, 5:2–5, 2006.

[17] W. Nelson, M.-C. Rosenberg, J. Weiss, and M. Goodrich. New Hampshire critical access hospitals: CEOs' report on ethical challenges. *Journal of Healthcare Management*, 54(4):273–83, 2009.

[18] A. J. Thomson and D. L. Schmoldt. Ethics in Computer Software Design and Development. *Computers and Electronics in Agriculture*, 30:85–102, 2001.

[19] U.S. Department Of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Center for Biologics Evaluation and Research. General Principles of Software Validation; Final Guidance for Industry and FDA Staff. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm085371.pdf, 2002. Retrieved January 15, 2010.

[20] U.S. Department Of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Center for Biologics Evaluation and Research. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089593.pdf, 2005. Retrieved February 11, 2010.

[21] World Health Organization, Eastern Mediterranean Regional Office. eHealth Code of Ethics. http://www.emro.who.int/his/ethicscode.pdf, 2000. Retrieved February 11, 2010.

[22] O. Zaiane. Electronic Health Record and Data Analysis. http://moodle.cs.ualberta.ca/course/view.php?id=228, 2010. Retrieved January 11, 2010.