EJLT European Journal of Law and Technology

A study to define the international guidelines of ethics concerning electronic medical data

Mohammed Jawad, [1] Elsa Butrous, [2] Benjamin Faber, [3] Chandni Gupta, [4] Christopher Haggart, [5] Patel [6]

Cite as: Jawad, M., Butrous, E., Faber, B., Chandni, G., Haggart, C., Patel, S., 'A study to define the international guidelines of ethics concerning electronic medical data', European Journal for Law and Technology, Vol. 3, No. 1, 2012

1. Abstract

There has been a global increase in the use of information systems, with a growing amount of electronic data being collected, stored, processed, manipulated, transferred and distributed (these being the four domains of usage). Medical data is no exception, with the explosion of Electronic Health Records (EHR) and healthcare data mining being key examples. Such activities have created an array of ethical dilemmas concerning the use of Electronic Medical Data (EMD). A preliminary literature review revealed a lack of universal, international and conclusive set of ethical guidelines pertaining to these domains of EMD. The following literature review helps fill this void by creating such a set of ethical guidelines.

2. Introduction

Moore's Law forecasted that computer power will double roughly every 12-18 months. [7] This speed of innovation has resulted in more affordable and powerful computers being available to the everyday consumer and such technological strides have been particularly apparent within the healthcare sector, where terabytes of EMD are created every year. [8] This study has taken EMD to mean:

> 'data taken from a source of healthcare or medical research which is then computed into a digital format where it can then be collected, stored, manipulated, processed, transferred and distributed by information technology'. [9]

Although the usage of information systems creates countless healthcare benefits, there are a number of personal and confidential ethical issues relating to the usage and transfer of details between healthcare professionals, payers and researchers. For instance, will the increase in EMD lead to unethical privacy and security infringements? An ideal compromise would be to maximise utility without compromising ethical rights.

The rise in data transmission and usage emphasises the need for comprehensive ethical guidelines, however a preliminary literature review revealed no such guidance. [10] Although governing ethical bodies have a critical role to play, the unique nature of EMD requires an additional approach: one beyond the services offered by these ethical bodies. [11] A comprehensive set of ethical guidelines provides this alternate approach.

There are a multitude of ethical principles that can help shape morally reasoned and logical arguments with regard to EMD usage. Therefore, this study's ethical discussion required an appreciation of classical ethical principles and an in-depth understanding of relevant literature. To achieve this, this study drew heavily on the ideas, beliefs and principles outlined by prominent authors to formulate the guidelines. [12] The study also acknowledged the existence of laws, religion and societal values which all play a part in shaping moral

principles, and thus ethical rules of conduct. [13] However, it is important to note that this study strayed away from linking the ethical guidelines to law which is inherently societal-based. [14]

3. Methodology

As this study found no specific tool for the formation of ethical guidelines, a customised framework specific to this study was required. A nine-stage process framework was created using key themes adapted from generic guideline development cycles. [15] [16]Stages I to VI were carried out, while stages VII-IX will form the basis of future work (See figure 1).

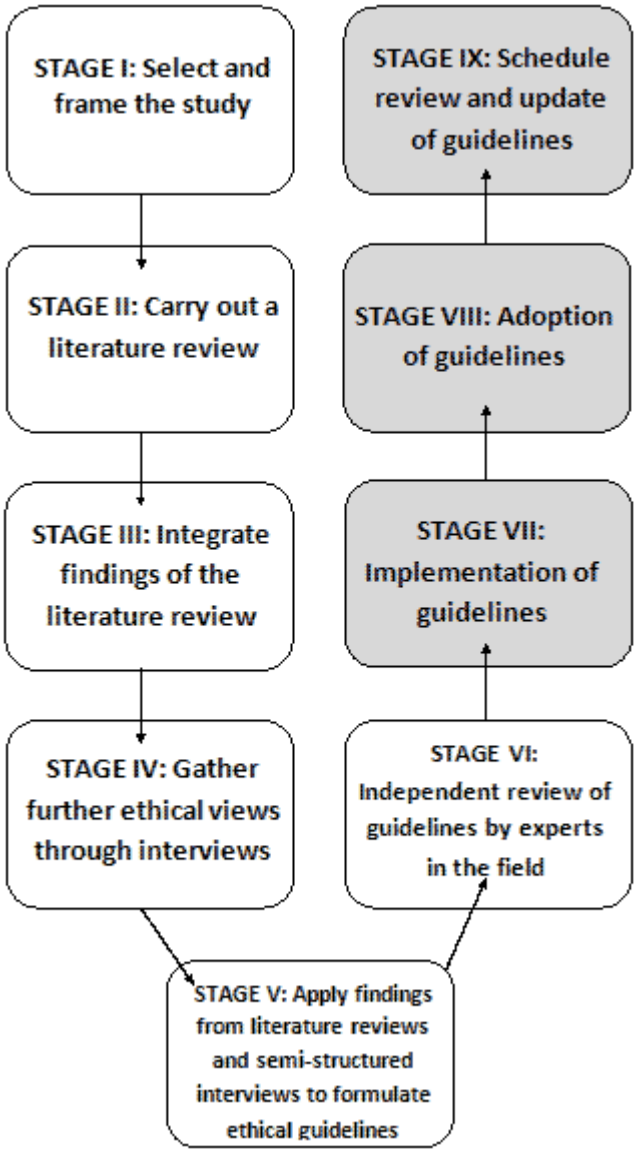

Table 1 Search terms

Anonymisation; confidentiality; consent; control; developing countries; distribution; duration of use; electronic; electronic health data; ethic; expiration of use; freedom of use; global; governance; guidelines; health data; informatics; information system; informed consent; international; law; legislation; manipulation; medical; medical information systems; OECD; ownership; privacy; protection; regulators; scope of use; security; transfer

Table 2 Inclusion/Exclusion criteria

Inclusion Critera
- Peer-reviewed papers, news articles, editorials, letters to journals and existing organisational ethical guidelines
- Ethical issues of paper medical data
- Non-medical literature
- Worldwide literature
- Literature with no citation numbers
- Older papers
Exclusion Criteria
- Literature focussing on the technicalities of electrica data usage
- Literature focussing on the law

Figure 1 Nine-stage diagram for developing ethical guidelines

Stage I involved selecting the topic of issue, which was the ethics of EMD. Aims and objectives were created and justified using existing literature. *Stage II* consisted of a comprehensive literature review including the selection and critique of papers. Search terms and inclusion/exclusion criteria (Tables 1 & 2) were used to standardise searches across a variety of online databases. Search techniques (e.g. truncation and snowballing) were incorporated. In *Stage III*, the findings of the literature review were merged into a coherent

manner revealing an important list of sub-issues: ownership, informed consent, accountability, security, privacy, anonymisation and access. This enabled cross-referencing with the original four domains of use.

Stage IV involved interviewing leaders in the field of medical ethics (see acknowledgements) to add further critique to our literature review. The interviews were semi-structured to evoke the interviewee's moral reasoning and ethical standpoints. *Stage V* required an amalgamation and critique of concepts raised during the literature review and interview process. Conclusions were deduced and summarised, creating approximately five to ten guidelines under the four domains of use. In *Stage VI* the guidelines were submitted to experts in the field of medical ethics for feedback and review (see acknowledgements). *Stages VII, VIII and IX* are beyond the remit of this study.

4. Discussion

The logic and reasoning behind the guidelines is discussed below.

4.1 Collection

This study defines the collection of EMD as 'the process of obtaining medical information so as to establish a factual basis for research and clinical decision-making'. [17] In the field of ethics it is not simply a matter of what type of data is collected and whether it is relevant, but also how it is collected and by whom. It is clear from the literature [18] and the views of all those interviewed that to ethically collect EMD where a patients' identity can be traced, one should obtain informed consent. [19] [20] Two interviewees believe that it is very difficult to achieve truly informed consent as it is almost impossible to convey the required level of understanding. Fully informed consent should be the ultimate ethical goal, but adequately informed consent will probably be the most feasible and still ethically acceptable alternative.

Informed consent also requires individuals to be aware of any possible uses of their data, termed the 'scope of use'. Annas believes that consent should be waived in certain circumstances, for example, by an independent body representing societal views. [21] In addition, there is a clear argument that securely de-identified data can be collected without consent provided there is a legitimate purpose. Obviously, it would be unethical to let any data be used for an unethical purpose; hence an independent body should have to legitimise the purpose. This leads to the following guidelines:

1. Ethical collection of patient identifiable electronic medical data should be carried out with informed consent and with direct consideration to the scope of use of data.

2. Where electronic medical data is anonymous or sufficiently de-identified, it is ethical to collect without consent when there is independent ethical approval for the use of that data.

The next guideline is based on the principle of privacy with a more detailed discussion found in the *Storage* section. [22]

3. Data collection should not exceed the necessary amount of electronic medical data required.

It follows that for a data subject to consent to the collection of their medical data, they must be able to fully understand what they are consenting to. Therefore, it is important that the data subject has the right to request further information about how their data might be used. The data collector should be sufficiently open and willing to explain to a data subject, the degree of data use.

4. Subjects have the right to request information pertaining to the scope of use of their electronic medical data.

5. Data collectors have an ethical responsibility to ensure the maximum feasible transparency.

Loshin identifies a list of parties which can lay potential claim to data including the creator, consumer, compiler, funder and purchasers. [23] Although each has a right to claim ownership, ownership does not necessarily place responsibility on them. The specified level of security laid out when collecting data should be maintained when managing the data. It is therefore the data collector's responsibility to make sure they collect the data under these conditions.

6. Those that collect the electronic medical data are ethically accountable for the data and to the persons on which it is based.

Clearly, as health care practices become more aligned with data storage, a certain degree of consent will be critical for receiving optimal care. A subject should be able to refuse collection of their EMD as it has been determined that obtaining consent is ethically sensitive. One interviewee discussed the importance of ensuring that these patients who do refuse consent are subsequently not treated in a biased nature. However, these subjects must also understand the possible disadvantageous consequences.

7. Subjects should not be additionally disadvantaged if they decline electronic medical data collection and should be adequately informed of the possible consequences of this.

4.2 Storage

As EHR's become commonplace, it seems reasonable for subjects to allow their information to be stored electronically, especially to ensure continuity of care. In the medical profession, this storage usually occurs under implied consent. Furthermore, if subjects have consented to data collection, then by implication, they have consented to its storage.

Duration of storage is another important variable of consent. It is ethically appropriate to clarify how long data should be stored: for example whether a subjects' EHR is being stored for life.

1. Data storage should occur with respect to appropriate consent from the subject, which should include the duration period of storage.

It is argued that only EMD that is necessary for the purpose of use should be stored. [24] [25] [26] This is based on the ethical reasoning that one should only store data that directly influences the greater good.

2. After electronic medical data is collected, only the relevant amount for the purpose should be stored.

The following guideline is justified by the argument that if a party collects the data, only they can directly control the data so they must be held accountable for its storage.

3. The party who collected and stored the electronic medical data should be held accountable for the safe storage of that data.

Trust is an 'ethical imperative' and it should be guarded by protecting privacy. One interviewee put forward privacy as one of the four key ethical principles in medicine because it not only maintains trust but upholds autonomy. [27] Privacy is achieved through maintaining adequate security. It is important that the security of data should not prevent timely access to data otherwise it may jeopardise the purpose of storing it (i.e. allowing access to an EHR in an emergency).

4. Electronic medical data should have an appropriate degree of security to safeguard subject privacy whilst allowing appropriate ease of access.

Security is designed to prevent unauthorised access. Therefore, ethically stored data should only grant access to those people with a legitimate purpose. [28] [29]

5. Only those parties with an authorised mandate for the use of the stored EMD should be granted access.

4.3 Processing and Manipulation

Informed consent is crucial within ethical processing and manipulation of EMD. A subject should provide consent for the manipulation and processing of their own EMD such as in data mining. The principle of openness helps one understand that consent should be given by the subjects every time the data is processed for a new purpose. [30] The deCODE case (where the biomedical company was granted permission to access the existing medical records database of all Icelandic people and create a genetic database) revealed concerns for neglecting the principle of autonomy by breaching privacy and consent. [31]

A further issue requiring discussion is the linking of non-casual events. [32] A potential ethical dilemma emerges when a researcher accesses and collates separate, unrelated electronic data sets pertaining to the same individual. This researcher may argue that this is perfectly ethical behaviour because on both counts, the subject has fully consented to the data being used for research. However, an unethical action could occur if these separate data sets are then analysed and combined to create a new data set: one that is sensitive to

the individual and developed without consent. There are obvious utilitarian benefits of data mining for research purposes. However, this argument does not justify that identifiable data can be freely manipulated and processed without consent.

1. Parties should ensure that informed consent is re-obtained if the original purpose of collecting the identifiable electronic medical data is modified and new information is created.

Electronic data storage and processing systems such as Healthvault or Google Health are increasing in number and power. It is a moral right to decide whether one wishes to consent to the inclusion in such a scheme, and thus reap the benefits from participating. However, professionals prefer a universal system for all subjects and often only one option is employed within organisations. Thus, the study has concluded that subjects should not receive any adverse effects than those already attributed to withholding consent, from data processing and manipulation systems.

2. Subjects should not be adversely affected if they choose not to accept the terms concerning the manipulation and processing of electronic medical data.

The ambiguity of who owns EMD causes difficulties in deciding who has the right to manipulate and change data. There is an egoistic right to amend your own data. However, from a utilitarian perspective, changes to EMD which could prevent benefits or even harm others should be challenged. For example, patients may remove their HIV positive status. This action can be described as an egoistic decision as the patient is attempting to maximise personal gains, irrespective of the impact on others. One of our interviewees believes that modifications to EMD should not be allowed for subjective, decision-making information such as diagnoses. Therefore, the changes one makes must be tracked and approved by those who are responsible for the data and its use.

3. Data subjects should have the right to access and request changes to their electronic medical data provided approval is granted from those who are accountable for the data.

It is particularly important to ensure that healthcare-related data is accurate and reliable. Processing and manipulation of EMD may lead to substantial errors which could have repercussions on the subject or on research. Some researchers go further and argue that there is an increased risk of duplicate entries if data is anonymised leading to unreliable and/or biased data, and so they argue that they should be able to use and manipulate data that has not been anonymised to the fullest extent even if they do not have consent. [33] Those accountable for data have a moral obligation to ensure that mistakes are avoided, and this study has also noted that only those accountable should carry out these checks in order to avoid privacy breaches. This quality assurance can be achieved through audits and reviews.

4. Manipulators and processors of electronic medical data should have an ethical responsibility to ensure accuracy and reliability of electronic medical data via regular audits and reviews.

Acts and laws are already in place to protect individuals from security and privacy breaches. However, the ethical implications of notifying a subject are considered further in this study. The organisation responsible for such a breach may fear negative publicity or financial repercussions, but the maintenance of a subject's respect and dignity is more ethically valuable. Therefore, the manipulator responsible has a moral obligation to rebuild the trust of the subject following a breach.

5. In the event of a data breach, manipulators and processors should have an ethical duty to inform the subject whose data security and privacy has been compromised.

Considering both Guideline 4 and 5, if a breach is detected, it follows on that an investigation into the causes must be carried out in order to reassure the subject and rebuild their trust for the manipulation and processing of EMD.

6. In the event of a data breach, manipulators and processors should have an obligation to ensure that they are able to conduct a sufficiently extensive review and audit, to identify the cause of a data breach.

As previously mentioned in Guideline 1, consent should be obtained for the access to identifiable EMD. Out of courtesy, consent for anonymised data should also be obtained but there is a general consensus that it can be manipulated and distributed without consent, especially for a utilitarian purpose. However, there are various degrees of anonymised data and thus manipulating and processing without consent is a minefield. Ideally, privacy should be maintained through de-identification but the study also appreciates that unreliable,

unhelpful and inaccurate information could result from de-identified data. Sufficient de-identification, as approved by an independent body, should be ensured during the manipulation and processing of EMD.

7. It is ethical to use unconsented anonymised electronic medical data for secondary use provided it has been adequately de-identified and its use reviewed by an independent ethical body.

4.4 Transfer and Distribution

The transfer and distribution of EMD internationally or between organisations, institutions or individuals raises ethical dilemmas. The requirement to gain informed consent is once again critical.

The example of data transfer and distribution from the N3 secure network to the unsecure internet requires ethical consideration. For instance, there is a need to inform subjects of such transfers and to gain informed consent, especially if data is of an identifiable nature. However, the argument against this is the potential hindrance to healthcare research and services if informed consent was required during transfer, or that there would be feasibility issues associated with gaining consent. One interviewee refused to accept that feasibility difficulties are an excuse for not gaining consent, but in an emergency, informed consent must be waived if this is in the patient's best interests. An overarching compromise could be to accept that the transfer and distribution of unidentifiable data is acceptable without consent, (as any potential security breaches are highly unlikely to result in subject identification).

A related argument is that consent should always be obtained for identifiable data. This stance is supported by EPSOS, a leading organization in the field of medical data transfer, who have stated a need to gain consent for international transfers, especially when EMD is identifiable. [34]

1. Adequate consent for a purpose should be obtained whenever identifiable electronic medical data is transferred and distributed.

2. Consent should not be required for the ethical transfer and distribution of de-identified electronic medical data.

3. When electronic medical data is transferred and distributed across borders or an unsecured network, informed consent should be obtained for this transfer and distribution.

The ambiguous relationship between ownership and accountability is apparent. One can conclude that the owner of the EMD has responsibility over the data set, which mirrors the Traditional Rule argument where the physician should also assume accountability. Alternatively, one could argue the data subject should maintain ownership of EMD, as it is information about them: a view which two interviewees also agreed with. An ethical conclusion arose that regardless of ownership, the party that transfers EMD should always maintain responsibility over it, rather than the owner of the data. This stance is supported by the PIPEDA guidelines. [35] However, the constantly developing worldwide web and IT pose difficulties in maintaining accountability over electronic data (as it can be transferred and distributed so quickly). A further relevant view is that regardless of standardisation and rules, there are always exceptions in the owner-decision maker relationship. In times of medical emergency, medical professionals may need to decide to transfer data even though the patient is the data owner, hence, a degree of leeway is required.

4. The party who are transferring and distributing electronic medical data should be accountable for the data.

5. The decision to transfer and distribute electronic medical data should be assessed on a case-by-case basis when the ethical owner of the data is in doubt.

Another ethical point of concern stemming from the sending party's obligations and accountability is the need for review and audit processes. As previously explained, the transfer and distribution of EMD is no longer a one-action situation, and there may be a requirement for audits and reviews before, during and after transfer or distribution. This is an argument adopted by PIPEDA who state the transferring organization should have the right to conduct such an audit of the receiving party. [36] However, alongside the ability to review and audit the receiver there is an ethical responsibility to maintain EMD security and privacy. This means there is also a long-term responsibility to conduct audit trails and ensure security, regardless of where EMD travels and gets distributed.

6. The sending party has an ethical obligation to review and audit the recipient's security status before, during and after electronic medical data transfer and distribution.

Security is a crucial topic of consideration with regard to transfer and distribution of EMD. As Surgenor mentions, technological developments have created 'more opportunities for potential unauthorized use and criminal acts'. [37] One option could be to set a minimum standard of security that must be met during EMD transfer and distribution. However, this is a potentially unethical action, not to mention highly unfeasible when considering the global variation in security measures. Therefore, a comparative approach to security seems to be the most ethically acceptable and feasible guideline, as it also ensures consistency with Rawls' generality principle. [38]

7. Data transfer recipients should provide equal or greater levels of security than the electronic medical data sender.

The appropriate level of encryption is a further requirement during data transfer and distribution, as it helps uphold the underlying ethical right for all individuals to expect a level of privacy. A discussion of encryption and privacy cannot occur without incorporating the closely related topic of de-identification. Complete anonymisation is the most ethically acceptable situation, however this is unrealistic. Therefore, a high level of de-identification is the most feasible alternative, as well as being ethical. Not only will this ensure a subject's privacy is maintained: it also provides researchers with significant room for research and data usage which goes some way to partially achieving utilitarian benefits. This is as long as de-identification has been achieved.

8. Electronic medical data should be encrypted when transferred and distributed.

9. Electronic medical data, when transferred and distributed, should have a maximum level of de-identification if consent has not been obtained.

5. Limitations and Future work

The guidelines were formed using a rigorous framework but this study accepts that the appraisal process was limited. Therefore, a key area for further work would be to receive appraisal from persons who implement ethical guidelines into practice. Such appraisal would further refine the guidelines. All interviewees were experts in the field of ethics and EMD and all based within the UK. However, for guidelines to be accepted internationally, they must have the support and critique of global leaders too.

6. Acknowledgements

The authors would like to acknowledge the following individuals: Dr Wing May Kong, Trustee of the Institute of Medical Ethics; Reader of Medical Ethics and Law at Imperial College London, Christopher Haggart Dr Michael Wilks, co-author of Medical Ethics Today; Chair of the BMA Ethics committee, 1997-2006, Helen Atherton, currently authoring and co-ordinating a suite of 5 Cochrane systematic reviews on email communication in healthcare; Clare Sanderson, Director of information governance at the NHS Information Centre,Lord Ara Darzi - Chair of surgery at Imperial College London; Author of the NHS Next Stage Review, 2008 and past parliamentary under-secretary of state in the Department of Health, Professor Raanon Gillon - Previous editor of the Journal of Medical Ethics; Emeritus Professor of Medical Ethics at Imperial College London

---

[1] Mohammed Jawad is a fourth year medical student at Imperial College London, intercalating with a BSc in Medical Sciences with Management at Imperial College Business School

[2] Elsa Butrous is a fourth year medical student at Imperial College London, intercalating with a BSc in Medical Sciences with Management at Imperial College Business School

[3] Benjamin Faber is a fourth year medical student at Imperial College London, intercalating with a BSc in Medical Sciences with Management at Imperial College Business School

[4] Chandi Gupta is a third year medical student at King's College London, intercalating with a BSc in Medical Sciences with Management at Imperial College Business School

[5] Christopher Haggart is a fourth year medical student at Imperial College London, intercalating with a BSc in Medical Sciences with Management at Imperial College Business School

[6] Sagar Patel is a fourth year medical student at Imperial College London, intercalating with a BSc in Management in Medical Sciences with Management at Imperial College Business School

[7] Moore, G. Cramming more components onto integrated circuits. Electronics 1965;38(8): 114-117.

[8] Safran, C., Bloomrosen, M., Hammond, E., Labkoff, S., Markel-Fox, S., Tang, P. C., Detmer, D. E. Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. *Journal of the American Medical Informatics Association*, 2007;14 (1): 1-9.

[9] Authors' own definition

[10] Freed-Taylor, M. Ethical considerations in European cross-national research. *International Social Science Journal* 1994;142: 523-532.

[11] Cios, K., Moore, W. G. Uniqueness of medical data mining. *Artificial Intelligence in Medicine* 2002;26(1-2): 1-24.

[12] In particular the following authors: Beauchamp, T. L., Childress, J. F. *Principles of Biomedical Ethics*. 5th Edition, Oxford: Oxford University Press;2001, Gillon, R. Medical Ethics: Four principles plus attention to scope. British Medical Journal 1994;309(6948): 184-188. , Mason, R. O. Four Ethical Issues of the Information Age. *Management Information Systems Quarterly* 1986;10(1): 5-12., Aroskar, M. Anatomy of an Ethical Dilemma: The Theory. *The American Journal of Nursing*1980;80(4): 658-660, Kluge, E.-H. W. Informed consent to the secondary use of EHRs: informatic rights and their limitations. *Studies in health technology and informatics* 2004;107(1): 635-638, Laudon, K., Laudon, J. *Management Information Systems*: Global Edition. 11th edition, Pearson Education;2009

[13] Tavani, H. T. *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing*. 3rd Edition, New Jersey: Wiley;2009

[14] Kluge, E.-H. W. Professional codes for electronic HC record protection: ethical, legal, economic and structural issues. *International Journal of Medical Informatics* 2000;60(2): 85-96.

[15] Browman, G. P., Levine, M. N., Mohide, E. A., Hayward, R. S., Pritchard, K. I., Gafni, A., Laupacis, A. The practice guidelines development cycle: a conceptual tool for practice guidelines development and implementation. *Journal of Clinical Oncology*1995;13(2): 502-12.

[16] Graham, I. D., Harrison, M. B., Brouwers, M., Davies, B. L., Dunn, S. Facilitating the use of evidence in practice: evaluating and adapting clinical practice guidelines for local use by health care organizations. *Journal of obstetric, gynecologic, and neonatal nursing* 2002;31(5): 599-611.

[17] Balanced Scorecard Institute. (n.d.) *Basic Tools for Process Improvement - Module 7 Data Collection*. [Online] Available from: http://www.balancedscorecard.org/Portals/0/PDF/datacoll.pdf [Accessed 10th May 2010]

[18] Annas, G. J. Medical privacy and medical research - judging the new federal regulations. *New England Journal of Medicine* 2002;346(3): 216-20.

[19] Kluge, E.-H. W. Informed consent to the secondary use of EHRs: informatic rights and their limitations. *Studies in health technology and informatics* 2004;107(1): 635-638.

[20] Annas, G. J. Medical privacy and medical research - judging the new federal regulations. *New England Journal of Medicine* 2002;346(3): 216-20.

[22] Buckovich, S. A., Rippen, H. E., Rozen, M. J. Driving Towards Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information. *Journal of the American Medical Informatics Association* 1999;6(2): 122-133.

[23] Loshin, D. *Knowledge Integrity, Inc.* [Online] Available from: http://knowledge-integrity.com/wpblog/ [Accessed 20th May 2010]

[24] Krishna, R., Kelleher, K., Stahlberg, E. Maintaining Patient Confidentiality and Use of Clinical Medical Databases. *American Journal of Public Health* 2007;97(4): 654-658.

[25] Lee, M. L., Gostin, L. O., Ethical Collection, Storage, and Use of Public Health Data: A Proposal for a National Privacy Protection. *Journal of the American Medical Association* 2009;302(1): 82-84.

[26] IMIA - International Medical Informatics Association. *The IMIA Code of Ethics for Health Information Professionals*. [Online] Available from: http://www.imia.org/pubdocs/Ethics_Eng.pdf [Accessed 7th May 2010]

[27] Mommens, P. Ethical Issues of healthcare in the information society. *Health Informatics Journal* 1999;5(4); 233-239.

[28] Krishna, R., Kelleher, K., Stahlberg, E. Maintaining Patient Confidentiality and Use of Clinical Medical Databases. *American Journal of Public Health* 2007;97(4): 654-658.

[29] Lee, M. L., Gostin, L. O., Ethical Collection, Storage, and Use of Public Health Data: A Proposal for a National Privacy Protection. *Journal of the American Medical Association* 2009;302(1): 82-84.

[30] Kluge, E.-H. W. Professional codes for electronic HC record protection: ethical, legal, economic and structural issues. *International Journal of Medical Informatics* 2000;60(2): 85-96.

[31] Hlodan, O. *For Sale: Iceland's Genetic History*. [Online] Available from: http://www.actionbioscience.org/genomic/hlodan.html [Accessed on 2nd May 2010]

[32] Custers, B. The Risks of Epidemiological Data Mining. In: Chadwick, R., Introna, L.D., Marturano, A. (eds.), Proceedings of the *Fourth International Conference on Computer Ethics - Philosophical Enquiry* (CEPE 2001), UK. Lancaster University; 2001.p. 61-70

[33] Kalra, D., Gertz, R., Singleton, P., Inskip, H. M. Confidentiality of personal health information used for research. *British Medical Journal* 2006;333(7560): 196-8.

[34] Wilks, Michael. Forensic Physician. (Discussion on Ethics of Electronic Medical Data, 17th May 2010)

[35] Office of the Privacy Commissioner of Canada. *Processing Personal Data Across Borders Guidelines*. [Online] Available from: http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf [Accessed 8th May 2010]

[36] Office of the Privacy Commissioner of Canada. *Processing Personal Data Across Borders Guidelines*. [Online] Available from: http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.pdf [Accessed 8th May 2010]

[37] Surgenor, V. The price of data sharing. *Network Security* 2006;2006(10): 8-10.

[38] Aroskar, M. Anatomy of an Ethical Dilemma: The Theory. *The American Journal of Nursing* 1980;80(4): 658-660.