eChallenges e-2010 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2010
ISBN: 978-1-905824-21-2

Ethical Implications of Digitised Medical and Biometric Data

Siang-Ting SIEW[1], Rohaya MOHD-NOR[2], Samantha SWARTZMAN[3], Terrin LIM[4], Benita COX[5], Alvin W. YEO[6], Zaharya MENEVIDIS[7]
[1, 2, 4,6]*Universiti Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia*
Tel: +60 82-581000, Fax: +60 82-665088
[1]*Email:* **s.siangting@gmail.com** , [2] **mnrohaya@gmail.com**, [4]**terrinlim@gmail.com**, [6] **awyeo09@gmail.com**
[3, 5]*Imperial College London, London SW72AZ, UK*
Tel: +44 (0)20 7589 5111, Fax: +44 (0)20 7823 7685
[3]*Email:* **s.wartzman@imperial.ac.uk**, [5] **b.cox@imperial.ac.uk**,
[7]*Fraunhofer-Institute for Production Systems and Design Technology IPK, Pascalstrasse 8-9, 10587, Berlin*
Tel: +49 (0)30 / 3 90 06-1 97, Fax: +49 (0)30 / 3 91 75 17
Email: **zaharya.menevidis@ipk.fraunhofer.de**

Abstract: In this paper, ethical implications of data collection, use and retention of medical and biometric data in biometrics and medical applications are identified. These implications are discussed in the context of five main ethical principles – privacy, confidentiality, security, property and ownership, and reliability and trustworthiness. In addition, to illustrate unethical uses of medical and biometric data, cases of misuse are described. Our research contributes to the European Union's FP7 ETHICAL project, which aims to promote international debate on ethical implications of data collection, use, and retention of biometric and medical data.

1. Introduction

New technologies for biometric identification, medicine, and information management provide opportunities in many areas such as scientific research, international security, economic advancement, and criminal or forensic investigations. Databases of these applications containing personal information are increasingly interoperable, allowing for data sharing across organisations and countries. While this accessibility has its applications and its advantages, there are ethical concerns associated with the utilisation and storage of personal, sensitive, and identifiable data such as medical or biometric data. In Iceland, for example, the government has collected genetic information as part of their national health database [1]. From the standpoint of medical doctors, it was argued that allowing a private company, called deCODE, to have access to the genetic data of Icelanders without the patient's consent breaches the trust and confidentiality between doctor and patient [2]. This case emphasises the importance of being aware of the ethical issues pertaining to possible exploitation of human biological data.

In this research, there are three objectives. Firstly, ethical principles involved in gathering, utilising, and storing medical and biometric data are identified; secondly, cases of data misuse that have already occurred and ethical dilemmas associated with these cases of misuse are analyzed. Finally, pertinent ethical implications are discussed.

In this paper, ethics is defined as a branch of philosophy dealing with morality and amorality. In this case, ethics should be distinguished from law, policy, agreements, and cultural mores. All of these may contribute to or reflect an ethical system, but they are not ethics by themselves. It is not our position that data collection, use, and retention are always unethical. Ethical decision-making sometimes involves balancing competing interests like

valuable research and life-saving measures in the case of medicine or the "greater good" and national security in the case of biometrics. In the case of medical and biometric applications, "data" are information about individuals' bodies (physical, physiological, and hereditary) or behaviour. As such, in this paper, "data" will always refer to personal, sensitive, and potentially identifiable information.

Our research investigation contributes to the European Union's FP7 ETHICAL project, which aims to promote international debate on ethical implications of data collection, use, and retention of biometric and medical data. The ETHICAL mission is to be an effective mechanism for societal partners' engagement in enhancing this debate in order to create a consensus and a roadmap towards a secure environment and, simultaneously, no compromise in human rights respect. In this paper, we aim to further stimulate debates and discussion, and engage a wide range of beneficiaries from both public and private entities, institutions and professionals such as researchers, clinical personnel, policy makers, medical and biometric data technicians, consumers and patients about the ethical implications, dilemmas and problems on data collection, use and retention in medical and biometric applications.

2. Methodology

Articles relevant to problems of data use were identified. In particular, articles from accredited sources such as medical publications and journals are considered. This search for documents was carried out using search engines such as Google and Google Scholar. To ensure a widespread coverage of perspectives, ETHICAL research consortium members also contributed to the collection of case studies and articles. In the search, key terms such as the following: "data privacy," "data confidentiality," "data security," "data ownership," "medical ethics," and "bioethics" were used in filtering the search results.

3. Five Main Ethical Principles

3.1 Privacy

Privacy is defined as "the right of individuals to be left alone and to be protected against physical or psychological invasion or the misuse of their property" and it also "includes freedom from intrusion or observation into one's private affairs, the right to maintain control over certain personal information, and the freedom to act without outside interference" (ASTM, 1997 cited from [3]:123). It is also acknowledged that in addition to the legal standpoint, cultural values and public opinions can also influence one's views on the privacy rights of individuals. In the context of biometric and medical applications, this principle is challenged when data are collected and distributed without informed consent. Further, ethical dilemmas may also arise in the situation where the data are linked to other information about a person, or is improperly distributed to or shared with third parties [4]. [5] argued that the biometric technologies that are becoming sophisticated and the future development of its data exchange protocols to promote interoperability standards can pose further threats and ethical dilemmas pertaining to protecting individuals' privacy rights. Similarly, the growing adoption of electronic medical record applications intensifies the debate on the need to enhance privacy protection [6].

3.2 Confidentiality

Confidentiality refers to "the status accorded to data or information indicating that it is sensitive for some reason, and therefore it needs to be protected against theft, disclosure, or improper use, or both, and must be disseminated only to authorised individuals or