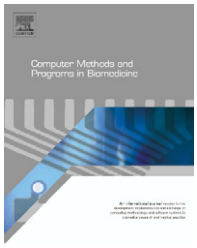
ELSEVIER

journal homepage: www.intl.elsevierhealth.com/journals/cmpb



Considering something 'ELSE': Ethical, legal and socio-economic factors in medical imaging and medical informatics☆

Penny Duquenoy[a], *Carlisle George*[a,*], *Anthony Solomonides*[b]

[a] *School of Computing Science, Middlesex University, The Burroughs, London NW4 4BT, United Kingdom*
[b] *CEMS Faculty, University of the West of England, Bristol BS16 1QY, United Kingdom*

ARTICLE INFO

Article history:
Received 7 January 2008
Received in revised form
14 May 2008
Accepted 3 June 2008

Keywords:
Ethical principles
Data protection
Confidentiality
Electronic medical data
Informed consent
Grid computing

ABSTRACT

The focus on the use of existing and new technologies to facilitate advances in medical imaging and medical informatics (MIMI) is often directed to the technical capabilities and possibilities that these technologies bring. The technologies, though, in acting as a mediating agent alter the dynamics and context of information delivery in subtle ways. While these changes bring benefits in more efficient information transfer and offer the potential of better healthcare, they also disrupt traditional processes and practices which have been formulated for a different setting. The governance processes that underpin core ethical principles, such as patient confidentiality and informed consent, may no longer be appropriate in a new technological context. Therefore, in addition to discussing new methodologies, techniques and applications, there is need for a discussion of ethical, legal and socio-economic (ELSE) issues surrounding the use and application of technologies in MIMI. Consideration of these issues is especially important for the area of medical informatics which after all exists to support patients, healthcare practitioners and inform science. This paper brings to light some important ethical, legal and socio-economic issues related to MIMI with the aim of furthering an interdisciplinary approach to the increasing use of Information and Communication Technologies (ICT) in healthcare.

1. Introduction

The benefits of utilising computer technology in medical practice have long been realised, and the risks of mediating healthcare using this technology have also been evident.[1] With the continuing rapid development of Information and Communication Technologies (ICT) in all sectors of society there have been key developments in the field of healthcare. A major focus of such technological use is in medical imaging and medical informatics (MIMI). Medical Imaging refers to a particular application area which focuses on techniques to create and analyse images of the human body (e.g. X-

☆ This article is an extension of a previous paper by the same authors: "What ELSE? Regulation and compliance in medical imaging and medical informatics" presented at MIMI 2007: Medical Imaging and Informatics Conference, Beijing, China, 15–16th August, 2007.

* *Corresponding author*. Tel.: +44 2084112726.
E-mail addresses: p.duquenoy@mdx.ac.uk (P. Duquenoy), c.george@mdx.ac.uk (C. George), tony.solomonides@uwe.ac.uk (A. Solomonides).

[1] The case of the X-ray machine Therac-25 with faulty software is an often cited example, see An Investigation of the Therac-25 Accidents by Nancy G. Leveson and Clark S. Turner. IEEE (1993) www.swqual.com/consulting/Therac25.pdf.

0169-2607/$ – see front matter © 2008 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.cmpb.2008.06.001

ray; ultrasound; magnetic resonance imaging, MRI; computed tomography, CT[2]) and is considered to play a crucial role in aiding medical diagnosis and planning a suitable treatment [1]. Image analysis is commonly used in medical processes such as the early detection of cancer, analysis of neurological disorders (e.g. stroke), monitoring the progress of cardiovascular disease and the response to treatment [2]. The term medical informatics encompasses the use of ICT and computing in the provision of healthcare generally. In all of these application areas computer technology intervenes between human actors by receiving information, processing it according to requirements, and delivering its results in new and useful ways. These processes occur within a context that is the domain of computer scientists, and within which the principles and governance procedures familiar to healthcare practitioners – and necessary to good healthcare practice – should be embedded. It is vital then for each of these professional domains to have a discourse that bridges the gap between the technical requirements and the ethical, legal and socio-economic requirements. This paper aims to promote this discourse by looking at how the core ethical principles behind medical practice make the transition to the digital domain, the significance of data protection legislation and the challenges posed, and how a changing technical infrastructure (the grid) reveals new and different challenges.

In pursuing our aims, we take as our focus the data that is the subject, and product, of the information process and which is used for various activities including clinical practice and research. This "electronic medical data" includes a wide range of data relating to a patient's health, including details of his/her past, current and future diagnoses, treatments and medication [3]. Electronic medical data also includes electronic/digital images such as an X-ray or mammography. Data processing includes collection, storage, organisation, retrieval, use, dissemination, consultation and transmission among others (EU Directive 95/46/EC). The processing of this data is critical since inaccuracies and misuse can have detrimental consequences for patients, medical professionals and researchers. Inaccuracies in a patient's medical data can result in misdiagnosis and medical professionals can face legal sanctions for malpractice due to inaccurate data; disclosure of medical data can result in prejudicial treatment and researchers can be criminally liable for unauthorised disclosure of medical data.

To protect electronic medical data and safeguard patients, medical professionals and researchers it is important that the ethical principles underpinning the medical profession, and the supporting legal measures are understood in the MIMI context. If there are failures in sustaining basic principles of patient protection the primary consequence results in harm to the patient, but we should also not forget the secondary consequence of a degradation of confidence in the healthcare system. ICT has the potential to bring enormous benefits to healthcare, but its use is also embedded in a socio-economic system and its impact in this respect must also be taken into account to ensure its viability and sustainability in the relevant domains. The discussion of ethical, legal and socio-economic (ELSE) issues related to ICT in healthcare is therefore important for the proper functioning of any healthcare system.

In the following pages we begin our discussion from the foundation of ethical principles that support healthcare, and the impact of technology on information relevant to patient care and ethics. We then turn to the formalisation of those principles in law, focussing on data protection legislation and issues relating to electronic health records. Finally we look at how the fundamental characteristics of technology – in this case the concept of Grid technology – require a reconsideration of the practical consequences of its use in respect of ELSE issues.

In all of these different contexts patient data may be used to inform direct diagnosis and treatment, or it may be aggregated into a database for research purposes. In both circumstances the integrity and quality of the data presented is equally important, but the different context of use (by practitioner or researcher) has different regulatory requirements. In the first instance, use by the practitioner, the data is retrieved from source (i.e. the patient) and is known as 'primary data'. In the second, the sets of data gathered for research purposes (which should be anonymised to protect patient confidentiality) are known as 'secondary data'. The regulations for primary and secondary data are presented in the section discussing legal issues within the scope of personal data and data used for research. The practical aspects of both are discussed in the final section that provides examples of two research projects, and demonstrates the challenges that Grid technology poses in meeting legal and ethical requirements.

2. Transforming ethical principles

In its capacity of supporting healthcare practice technology should also embody, or at least support, the core ethical principles of the medical profession. In western medicine these are founded on the Hippocratic oath which promises to honour the profession (and further knowledge), to keep patients from harm and injustice and respect patient confidentiality. In terms of medical informatics today we can say that the systems we use should support research (further knowledge), protect the patient from harm and provide care based on equality, and show respect to the patient by ensuring patient data remains confidential. These basic ethical duties are reflected in the principles put forward by Beauchamp and Childress [4] for the field of biomedical ethics as follows:

- Beneficence
- Non-malfeasance
- Autonomy
- Justice

Similar principles provide the foundation for research ethics[3] (i.e. the ethical conduct of research involving human

[2] CT (computed tomography) involves the use of computers to generate a 3D image from flat (i.e, 2D) X-ray pictures.

[3] Department of Health, Education, and Welfare, Office of the Secretary, Protection of Human Subjects. Belmont Report: Ethical

subjects) which is also strongly linked to medicine.

- Respect for persons (i.e. acknowledging individual autonomy, choices)
- Beneficence (i.e. promoting well-being, reducing risks, protection of participant)
- Justice (i.e. equal benefits to all involved)

As we have noted above, patient information collected and stored in digital format covers a range of aspects that: identify the patient, record symptoms, diagnosis, treatment, and relevant supporting evidence (such as medical images). Professionals interacting directly with the patient and supporting technology, such as radiologists in the case of X-rays, must protect patients from any adverse effects. Because of the clear risk to patients regarding radiation it is not surprising that there are codes of ethics in place (cf. the Radiation Therapist Code of Ethics[4] and Guidance on Safety[5]).

These are crucial ethical considerations that have, quite rightly, been addressed and are well documented. But radiation impact is not the only harm that can occur through the use of medical imaging as an aide to diagnosis, ongoing treatment, or research. The mediating effect of technology plays an important role, not only through capturing data and re-presenting it, but also in its capability of changing, storing, and disseminating information in ways that may either affect its interpretation, or be interpreted differently by different audiences. This applies to any patient-related information however it is represented—text, numbers, graphs, or images. Where the practice of medicine is mediated through technology, the professionals dealing with the technology play an important and associated role.

2.1. *Ethical principles and the IT profession*

The IT (information technology) sector is made up of different disciplines, which in broad terms might be categorised as electrical engineering, computer science, and information management. Again, in broad terms, ethical principles of these professions usually fall within groupings that protect the public interest, uphold the standards of the profession, promote knowledge transfer, and require a commitment to personal integrity. An overview of the principles embodied in codes of ethics and practice across the range of disciplines is beyond the scope of this paper, but of direct relevance are 'rules of conduct' for Health Informatics Professionals (HIPs) [5]. In the following paragraphs some specific principals designed for the Health Informatics Professional that pertain to medical data are discussed.

The fundamental ethical principles providing the foundation for Health Informatics follow those given in the previous section. They are: Principle of Autonomy; Principle of Equality and Justice; Principle of Beneficence; Principle of Non-Malfeasance; Principle of Impossibility (this latter principle bears on the assumption that it must be possible to meet the rights and duties expressed by the previous principles).

Taking the fundamental principles expressed above it is possible to derive more focused principles for the informatics setting which centre on privacy and associated personal data issues. In broad terms the privacy-related principles follow the principles laid out under EU data protection legislation (discussed further in the following section: legal issues). In more specific terms and in the context of this paper, Health Informatics Practitioners "have a duty to ensure that appropriate measures are in place that may reasonably be expected to safeguard:

- the security of electronic records;
- the integrity of electronic records;
- the material quality of electronic records;
- the usability of electronic records;
- the accessibility of electronic records."[6]

Taking the above points and transferring them to the context of medical imaging, we are adopting the position that the content (data) of medical images constitute an electronic record, and are personal data in that they represent information concerning a person (by virtue of the image and by virtue of its description embedded in the electronic file). However, this is not simply a discussion of personal data, and the rights of patients in connection with their data. It extends to issues of integrity and the interpretation of data.

2.2. *Transferring the ethical principles to context of use*

The five characteristics of electronic records listed above are clearly regarded by Health Informatics Professionals as important in the furtherance of healthcare and worth noting because each of them describe a state of usefulness that could be compromised through technical mediation. In simple terms these could be described as the 'crisis points' of technically mediated patient information. The aim of presenting patient information can be summarised as "the correct information at the right time, to the right people" which, for the purposes of the intention behind medical imaging, forms the basis for a strong ethical foundation. One only needs to consider the effects of the opposite – incorrect information at the wrong time, to the wrong people – to understand the importance of this. It should be noted that any combination of these aspects would result in an unwanted outcome (for example, correct information at the right time to the wrong people).

Principles and Guidelines for the Protection of Human Subjects of Research. Report of the National Committee for the Protection of Human Subjects of Biomedical and Behavioural Research. DHEW Publication No. (OS) 78-0013 and No. (OS) 78-0014. 18 April, 1979.

[4] American Society of Radiologic Technologists, available from: http://www.asrt.org/content/RTs/CodeofEthics/Therapy_CodeOfEthics.aspx.

[5] See for example the now complete European project Dimond at: http://www.dimond3.org/.

[6] The points listed are extracted from the handbook, and represent only a small portion of the complete book, they have been chosen for their specific relevance for the purposes of this short paper.

Table 1 – Relevant derivations of principles for Health Informatics Professionals and their interpretations

Security	To protect patient confidentiality (i.e. privacy) and integrity of the data
Integrity	The extent to which there is faithful reproduction of the original data source
Material quality	The extent to which a realistic interpretation can be made (i.e. related to image quality)
Usability	The ease with which the IT/human mediation can be made (without detriment to purpose)
Accessibility	The boundaries of access, the timeliness of access, and the presentation of material in a way that is accessible to those who need it

The following table provides an interpretation of the five 'crisis points' in relation to medical imaging (Table 1).

2.2.1. *Security*

The issue of security is relevant to this discussion in two ways. The first is that security in this instance relates to privacy and the maintenance of patient confidentiality. Secondly, securely held data is less liable to unknown or unwarranted human interference and therefore more liable to maintain its integrity. Both of these dimensions are included in the next section where the legal protection of personal data is covered in more detail. Suffice it to say here that the ethical dimension is that of patient confidentially.

2.2.2. *Integrity*

The integrity of the data does not solely depend on levels of security. The integrity of the data concerns its relationship to its source—in particular that it actually relates to the person it claims to relate to, and that it has not changed in a way that could cause harm to that individual. That is, the image used should have a provenance directly related to the patient and not have been interfered with. However, the technical mediation and transmission may, of necessity, interfere with the original mapping which may in turn have an impact on all the other aspects.

2.2.3. *Material quality*

Clearly the material quality of the image is important in order to be able to correctly identify any health issues, or to read associated and relevant text. Any ambiguity in the image (for example, caused by blurring, missing elements, etc.) may be detrimental to diagnosis, or other judgements—for example comparisons with other images for research purposes. Technical constraints of compression, reductions or enlargements of images may in some way add to material quality, but may have a detrimental affect on the other aspects of quality, usability and accessibility.

2.2.4. *Usability*

Some technical changes to the image may be necessary to aid usability. For example, compression to allow storage, or transmission, and subsequent decompression allow the exchange and sharing of data between users and across systems. Compatible file formats are important to reduce the need for more technical adaptations and risk of altering the quality and material content.

2.2.5. *Accessibility*

Accessibility and usability are of course linked to each other in terms of placing the 'human factor' within the scope of a successful 'human computer interaction'. The technical mediation of the image described although benefiting usability is likely to impact on accessibility, either beneficially (in the case of file sharing) or detrimentally. The enlargement of images, or changes in definition, for example may create difficulties when 'accessed' by their human interpreter (see e.g. [6]). Accessibility may not simply be a question of whether the image is physically accessible to whoever needs to see it at the time it needs to be seen. Cultural influences (not only national cultures but also work cultures) could prevent easy access. For instance, radiologists may be trained to interpret images presented in a different way, and may need training if they are presented in novel forms. Different approaches to medicine as practiced by different cultures may affect the perspective of the interpretation, or the ability to interpret. (Note the different approaches of eastern and western philosophies of medicine.)

It should be clear from the above discussion that the overriding aims of medical imaging meet the fundamental principles of beneficence, non-malfeasance, autonomy, and justice. That is, the aims of the endeavour are to increase human well-being and not do harm (in aiming for improvements in imaging and understanding the medical condition of an individual), and to share knowledge in pursuance of those aims (meeting the justice criteria). Autonomy as a principle acknowledges individuals as having the right to make choices, and not to be used as "means to an end". Providing that patients are given a choice (duly informed) in having an image made in the first place, and that the images used for research do not treat the individual simply as a statistic and ignore their individuality—then the 'autonomy' principle is met.

The mediating role played by technology, and the developments continuously being achieved in the field, can allow changes that may impact on these principles. The perspective taken here is essentially one of how computer technology is implemented to 'make life better', but that in order to achieve that objective consideration must be given to the context within which it is used—including scale and interconnectedness. Experience has shown that not only can new technologies offer a new, often more efficient, way of doing things they also offer a different context and concepts which are often difficult to understand (e.g. [7]).

This adaptation to new contexts, and the impact new contexts have on methods of working, are illustrated by the discussions in the next two sections. In the next section the transferring of patient records to the digital domain are highlighted by legislation on data protection (EU and UK) and the issues arising from the proposed introduction of electronic patient records using in the UK are discussed. The technological move into grid computing changes the context once again (in terms of where the electronic data is held), and this is discussed in the section on grid computing.

3. Legal issues regarding electronic health data

The proliferation of electronic medical data has undoubtedly resulted in significant benefits (e.g. enhanced patient autonomy, better clinical treatment, and advances in health research), however, there are also important legal challenges such as: the privacy of health information; reliability and quality of health data; and tort-base liability [8]. These are also interconnected because the degree of privacy protection determines the reliability and quality of the data, which in turn determines tort-based liability for acts such as malpractice (e.g. due to inaccurate data) or privacy invasions (e.g. unauthorised access, modification or disclosure) of data [8].

This section of the paper discusses legal issues relevant to electronic medical data used for two main purposes namely: clinical practice and medical research. In clinical practice data is used to make diagnoses, decide on treatment and monitor such treatments. In medical research, data is used in order to analyse, investigate and develop new treatments and techniques to advance medical practice.

The European Union data protection directive (EU Directive 95/46/EC) which forms the basis for data protection legislation in EU member states, will be used as an example of a legal framework which regulates medical data. Reference will also be made to the UK implementation of the EU Directive (The Data Protection Act 1998). The paper will also discuss the UK common law tort of breach of confidence.

3.1. *Data protection*

The EU Directive 95/46/EC sets out the legal framework for legislation in EU member states to regulate the processing of personal data.

In Article 2(a), the Directive describes personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" medical data therefore clearly falls within this definition.

Processing of data refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." Article (b).

Under the Directive, information about the physical or mental health or condition of an individual (i.e. medical data) is classed as a special/sensitive category of data and hence is given a higher level of protection.

The Directive stipulates data protection principles which must be observed (subject to various exemptions) when processing personal data, namely that personal data shall be (Article 6):

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes of processing;
- accurate and kept up to data;
- kept for no longer then necessary.

The UK Data Protection Act 1998 which implements the EU Directive lists additional data protections principles gathered from the spirit of the Directive namely that personal data shall be:

- processed in accordance to rights of data subjects;[7]
- kept secure from unauthorised access, unlawful processing, destruction or damage;
- transferred to a country outside the EU only if that country has an adequate level of data protection.

The UK Data Protection Act 1998 also specifies at least nine criminal offences relating to the failure to comply with provisions of the Act. These include: processing without notification to the Information Commissioner[8] (Section 21(1)); unlawfully obtaining or disclosing personal data (Section 55(1)); and unlawfully selling personal data (Sections 55(4) and (5)).

In addition to the data protection principles, the EU Directive prohibits the processing of data concerning health or sex life (i.e. medical data as a special category of data) except under the following exemptions (and any other exemptions laid down by member states) (Article 8):

- the data subject has given explicit consent[9] to the processing his/her data;
- processing is necessary to carry out the obligations and rights on the data controller in the field of employment law;
- processing is necessary to protect the vital interests of the data subject or another person where the data subject is not capable (physically or legally) of giving his/her consent;
- processing is carried out in the course of the legal activities of a foundation, association or non-profit seeking body

[7] The Act gives data subjects (who are the subject of personal data) various limited rights in Part II such as the right of access to personal data subject to exemptions for example, if in the opinion of a relevant health professional such access would result in serious physical or mental harm to the data subject or any other person (*The Data Protection* (*Subject Access Modification*) (*Health*) *Order* 2000).

[8] Section 17 of the UK Data Protection Act 1998 requires that all data controllers must register with the Information Commissioner and give notification of his processing activities. The Information Commissioner is the official responsible for supervising the enforcement of the Data Protection Act.

[9] Consent means that the data subject gives his/her agreement to process his personal data. Consent must be informed, the person giving consent must have a degree of choice, and consent must be indicated either in an express manner (e.g. explicitly—orally or in writing) or it must be implied.

(with political, philosophical, religious or trade union aims), on the condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data were not disclosed to the third party without the consent of the data subjects;
- the processing is necessary for medical purposes (preventative medicine, medical diagnosis, medical research, treatment and healthcare management) and is undertaken by a health professional or a person who is under an obligation of confidentiality/secrecy similar to a health professional.

Regarding data used for research, the EU Directive empowers member states to exempt certain provisions of the Directive. For example, the UK implementation of the EU Directive, (the Data Protection Act 1998) gives special provisions for research purposes (which includes statistical or historical purposes) subject to compliance with 'the relevant conditions' (Section 33 of the UK Act) namely that: personal data are not processed in order to make decisions regarding the data subject, and will not cause damage or cause substantial distress to any data subject. Under section 33(2) of the UK Act data processed for research purposes (subject to compliance with 'the relevant conditions') are exempted from part of the second data principle, meaning that data not originally collected for research purposes, can be used for research, however, data subjects should be informed (due to the fair processing requirement) provided that contacting them does not involve a disproportionate effort.[10] In practice when collecting data from patients, they should be informed that their medical data may be used for treatment and research purposes (in order to provide better medical care). Under Section 33(3) of the UK Act, (subject to compliance with 'the relevant conditions') data processed only for research purposes are exempted from the fifth data principle, meaning that such data can be kept indefinitely. Further, Section 33(4)(b) of the UK Act allows for the publishing of research data provided that the data does not identify any data subject (i.e. it is anonymised).

3.2. *Confidence: duty and breach*

The law imposes a duty of confidence on anyone who receives information which he/she knows or ought to know should be regarded as being confidential. Information is deemed to be of a confidential nature (and hence attracts legal protection) if imparted in circumstances where there is an obligation of confidence between the parties (e.g. between medical practitioner and a patient). Medical data undoubtedly qualifies as confidential information. Medical professionals and researchers therefore have a 'duty of confidence' that obliges them not to disclose any medical information divulged to them unless authorised to do so. Disclosure will be authorised where the patient gives consent to disclosure or where disclosure is dictated by law such as in judicial proceedings or by statutory authority. Unauthorised disclosure of confidential information can result in the common law tort action of "breach of confidence" or in some circumstances negligence.

In the UK, the conditions for establishing a "breach of confidence" action were formulated in Coco v A N Clark (Engineers) Ltd. [1969] RPC 41 and requires namely that: there is information of a confidential nature (e.g. medical data); which was imparted in circumstances importing an obligation of confidence (e.g. between patient and medical professional) and there has was unauthorised use causing detriment (e.g. pain, suffering, public humiliation) to the party who originally imparted the information. A third party who receives information resulting from a breach of confidence also has a duty of confidence if he/she is aware or ought to be aware of the breach. An action in negligence can also result from a breach of the duty of confidence. For example where a medical professional or establishment fails to take reasonable care (e.g. adequate security) to prevent the disclosure of confidential information, and such disclosure results in injury (physical or psychological) to a patient.

It is worthwhile to note that The Health and Social Care Act 2001 (Section 60),[11] gives the Secretary of state the authority to temporarily suspend the duty of confidentiality (but not the Data Protection Act 1998), so that medical records can be used (without the consent of patients) for specified medical purposes where it is necessary or expedient to improve patient care or where there is an overriding public interest. Hence under Section 60, medical records can be used to carry out clinical audits, record validation and research without obtaining the consent of patients [9]. The rationale for Section 60 is that in some cases: consent cannot be obtained; it is impractical to obtain (e.g. where there are tens of thousands of patients); or excluding patients who refuse consent may devalue the data collected due to sample bias. In practice researchers need to apply for Section 60 exemption from the Patient Information Advisory Group,[12] of the Department of Health.

The issue of whether there is an overriding public interest needs to be made on a case by case basis, and can take into consideration factors such as the prevention of serious harm or abuse to others, national security, and the detection or investigation of criminal activity among others. Three court judgements in the UK regarding issues of disclosure of medical information to the public may shed some light on how the courts weigh the interest of the public against the duty of confidentiality.

In X v Y [1988] 2 ALL ER 648, the Court of Appeal prevented a national newspaper from publishing the names of two practising doctors suffering from AIDS. The Court concluded that: the risk of transmission of HIV from doctor to patient was minimal; there was a greater public interest in preserving the confidentiality of hospital records; and the information would

[10] A 'disproportionate effort' is determined on a case-by-case basis, taking into account factors such as the nature of the data, the time and cost involved in providing information to the data subject, and the effect on the data subject.

[11] The Health and Social Care Act 2001 (Section 60) [12] http://www.opsi.gov.uk/ACTS/acts2001/10015–g.htm#60.

[12] http://www.advisorybodies.doh.gov.uk/piag/Index.htm.

be of minimal significance to the public in view of the wide ranging public debate on AIDS. In W v Edgell [1990] 1 ALL ER 835, a court considered whether a doctor who had sent confidential information (about the mental health of a dangerous patient) to the medical director of another hospital and to the Home Office, had breached the patient's confidentiality. The court held that the public interest (protection from a dangerous criminal) justified the breach of confidence. Finally, in H (A Healthcare Worker) v Associated Newspapers Ltd. & Ors [2002] EWCA Civ 195 the Court of Appeal prevented the public disclosure of the identity of a doctor who ceased medical practice after being diagnosed as HIV positive and suffering from AIDS. The Court of Appeal stated that "there is an obvious public interest in preserving the confidentiality of victims of the AIDS epidemic and, in particular, of healthcare workers who report the fact that they are HIV positive".

Two of the cases above illustrate that the public interest is not always best served by public disclosure. With regards to the cases on HIV-infected health workers, maintaining confidentiality encourages workers who are infected in the future to identify themselves and seek treatment, hence preventing further harm to the public.

3.3. *Protecting electronic medical data in practice*

A main cause of concern regarding electronic medical data is that such data is protected from unauthorised processing (especially unauthorised disclosure, alteration and use). A research study into the public reaction to implementing a UK Integrated Care Record Service (ICRS) to allow the electronic sharing of medical data (among health carers and patients) concluded that the only barrier to accepting ICRS was the perception that security of electronic systems was an issue [10]. Another study investigating the impact of the UK Program for IT (NPFIT[13]) in primary healthcare, on clinicians and medical staff, found that the biggest concern was the issue of patient confidentiality and security of electronic records [11].

In order to allay the fears of medical professionals and patients (regarding privacy), adequate measures (in addition to network security) must be in place to ensure compliance with data protection legislation, and the common law duty of confidence.

In the UK, with the introduction of the National Health Service (NHS) Electronic Card Record (in spring 2007) the Department of Health adopted various practices for the implementation and operation of this new healthcare system. These practices were approved by the Information Commissioner as being consistent with the requirements under data protection legislation [12]. The process begins with the uploading of information regarding a patient's current medication, known allergies and adverse reactions into a database to form a Summary Care Record (SCR). All patients will be notified before uploading of their SCR and given the option: to decline one; limit the future scope of information in the SCR or to view the contents before uploading. The SCR, however will be uploaded without the explicit consent of the patient (but subject to notification and an opportunity to respond). After uploading, patients can remove any or all information uploaded to the SCR, and any subsequent additions to the SCR must be agreed between the patient and his/her doctor. Patients will also be able to limit the information which can be made visible without their consent. A wide-range of access controls have also been adopted. Only staff with a legitimate relationship with a patient will be able to access that patient's SCR.[14] All access to an SCR will be via a smartcard and PIN, and is logged (providing an audit log). All patients will be able receive a copy of the audit log giving details of access to their SCR. The NHS also guarantees that information in the SCR will not be shared with any organisation without the explicit consent of the patient.

With specific regard to confidentiality, Since November 2003 the NHS published a Code of Practice on Confidentiality [9] which sets out practical guidance for all workers within or under contract with the NHS. The Code uses a model which is aimed at providing a confidential service. This model has four requirements namely to: protect – patient's information; inform – patients of information use; provide choice – to a patient regarding disclosure or use of information and improve – the preceding three requirements.

The NHS also maintains a register of senior staff (healthcare or social professionals) who are responsible for protecting patient information called Caldicott Guardians.[15] The main responsibilities of a Caldicott Guardian are [13]: strategy and governance – championing confidentiality issues at the management level; confidentiality and data protection expertise, internal information processing – ensuring that confidentiality issues are reflected in organisational policies, strategies and procedures; and information sharing – overseeing arrangements, protocols and procedures for information sharing between organisations both external and internal to the NHS.

One of the challenges of protecting electronic data is that such data sometimes needs to be shared amongst organisations in order to assist medical professionals and researchers in making analyses, comparisons and deciding on diagnoses. Epidemiology[16] also occasionally requires larger or less uniform data sets than may be available from a single source. An example of this is in grid computing, which utilises many computers sometimes spread across organisations and geographical locations. The next section examines this aspect and discusses some of the ethical, legal and socio-economic issues related to grid computing.

[13] NPFIT includes care record systems, electronic booking service, electronic prescriptions and a national network infrastructure.

[14] This includes medical staff acting in an emergence such as staff working in an Accident and Emergency Department.

[15] Caldicott Guardians are named after Dame Fiona Caldicott who chaired a 1997 report of the Review of Patient-Identifiable Information (called The Caldicott Report).

[16] The study of factors affecting health and illness in different groups of people. It is concerned with how often these diseases occur and why.

4. Grid computing: ethical, legal and socio-economic issues

4.1. *Healthgrid*

Grid computing ('the grid') is a new paradigm of distributed computing, offering rapid computation, large scale data storage and flexible collaboration by harnessing together the power of a large number of commodity computers or clusters of other basic machines. The grid was devised for use in scientific fields, but has also been used in a number of ambitious biomedical applications, while applications to healthcare have been explored in research projects. There is some tension between the spirit of the grid paradigm and the requirements of medical or healthcare applications. The grid maximises its flexibility and minimises its overheads by requesting computations to be carried out at the most appropriate node in the network; it stores data at the most convenient node according to performance criteria. On the other hand, healthcare institutions are required to maintain control of their confidential patient data and to remain accountable for its use at all times. The ideal grid has been envisaged as the servant of a new collaborative paradigm, providing services to users who may, from time to time, join the grid, do some work and then leave, so that the transient alliances they form in their endeavours might be described as 'virtual organizations' or VOs for short. One approach to organizing the infrastructure for such collaboration is as a so-called 'service-oriented architecture' (SOA). In effect, it means that needed services – software applications – once constructed, are provided with a description in an agreed language and made available, or 'published', to be 'discovered' by other services that need them. A 'service economy' is thus created in which both ad hoc and systematic collaborations can take place. Medical data requires careful handling. Among the services required by healthcare applications are 'fine grained' access control – e.g. through authorization and authentication of users – and privacy protection through anonymisation or pseudonymisation of individual data or 'outlier' detection and disguise in statistical data. Despite this apparent conflict in requirements, certain characteristics of the grid provide the means to resolve the problem: in the spirit of this paradigm in which "virtual organisations" arise ad hoc, "grid services" may negotiate ethical, legal and regulatory compliance according to agreed policy. In this section, we wish to discuss the implications of such advances in the ELSE domains in part through reference to two EU-funded healthgrid projects.

4.2. *Breast cancer*

Areas of medicine and healthcare in which large databases – in both senses: with large numbers of records, and with large, multi-format records – are reasonable candidates for healthgrid applications. We consider one such example, the MammoGrid project, in the field of breast cancer.

Breast cancer is arguably the most pressing threat to women's health. For example, in the UK, more than one in four female cancers occur in the breast and these account for roughly 18% of deaths from cancer in women. Coupled with the statistic that about one in four deaths in general are due to cancer, this suggests that nearly 5% of female deaths are due to breast cancer. While risk of breast cancer to age 50 is 1 in 50, risk to age 70 increases to 1 in 15 and lifetime risk has been calculated as 1 in 9. The problem of breast cancer is best illustrated through comparison with lung cancer which also accounted for 18% of female cancer deaths in 1999. In recent years, almost three times as many women have been diagnosed with breast cancer as with lung cancer. However, the 5-year survival rate from breast cancer stands at 73%, while the lung cancer figure is 5% [14]. This is testament to the effectiveness of modern treatments, provided breast cancer is diagnosed sufficiently early. The statistics of breast cancer diagnosis and survival provide a powerful argument in favour of a universal screening programme. However, a number of issues of efficacy and cost effectiveness limit the scope of most screening programmes. The method of choice in breast cancer screening is mammography (breast X-ray). However, in younger women, the breast consists of around 80% glandular tissue which is dense and largely X-ray opaque. The remaining 20% is mainly fat. Through the menopause, this ratio is typically reversed. Thus in women under 50, signs of malignancy are far more difficult to discern in mammograms than they are in post-menopausal women. Consequently, most screening programmes, including the UK's, only apply to women over 50.

Electronic formats for radiological images, including mammography, together with the fast, secure transmission of images and patient data, potentially enables many hospitals and imaging centres throughout Europe to be linked together to form a single grid-based "virtual organization". While technological possibilities are co-evolving with an appreciation of their potential uses, it is generally agreed that the creation of very large "federated" databases of mammograms, which appear to the user to be a single database, but are in fact retained and curated in the centres that generated them would yield several benefits in better diagnosis and epidemiology. Each image in such a database would have linked to it a large set of relevant information, known as metadata, about the woman whose mammogram it is. Levels of access to the images and metadata in the database would vary among authorized users according to their "certificated rights": healthcare professionals might have access to essentially all of it, whereas, e.g., administrators, epidemiologists and researchers would have limited access, protecting patient confidentiality and in accordance with European legislation.

This scenario raises some obvious and some rather subtle questions of ethics and regulatory compliance. Informed consent, in the usual sense of the term, cannot encompass uses of data which cannot be foreseen at the time the consent is being given. On the other hand, unconstrained consent is not even possible in some countries. And yet, the value of this approach lies precisely in what medical researchers may discover through extending their research questions as they analyse the data at their disposal. How to resolve this dilemma? It would appear that the best a healthgrid researcher can hope for is to highlight some valuable uses which are currently precluded and to look for political change.

A somewhat less obvious question concerns rights of access and confidentiality. How to reconcile, e.g. legal differ-

ences in what data a doctor may view in one country versus another? Does the constraint apply to an individual irrespective of their location or does it apply to a location? In other words, may a Scots doctor possibly view some data about her Scots patient (who has had some intervention in England) while visiting an English hospital which she would not be allowed to view in Scotland? What if that data is available to be viewed over a grid?

4.3. *MammoGrid project*

The fifth framework EU-funded MammoGrid project (2002–2005) [15] aimed to apply the grid concept to mammography, including services for the standardization of mammograms, computer-aided detection (CADe) of masses and 'microcalcifications', quality control of imaging, and epidemiological research including broader aspects of patient data. Clinicians rarely analyse single images in isolation but rather in a series or in the context of metadata. Metadata that may be required are clinically relevant factors such as patient age, exogenous hormone exposure, family and clinical history; for the population, natural anatomical and physiological variations; and for the technology, image acquisition parameters, including breast compression and exposure data.

The MammoGrid proof-of-concept prototype provides clinicians with a medical information infrastructure delivered in a service-based grid framework. It encompasses geographical regions with different clinical protocols and diagnostic procedures, as well as lifestyles and dietary patterns. The system allows, among other things, mammogram data mining for knowledge discovery, diverse and complex epidemiological studies, statistical analyses and CADe; it also permits the deployment of different versions of the image standardization software and other services, for quality control and comparative study.

We may now imaginatively consider what may happen in the course of a consultation and diagnosis using the MammoGrid system. A patient is seen and mammograms are taken. The radiologist is sufficiently concerned about the appearance of one of these that she wishes to investigate further. In the absence of any other method, she may refer the patient for a biopsy, an invasive procedure; however, she also knows that in the majority of cases, the initial diagnosis turns out to have been a false positive, so the patient has been put through a lot of anxiety and physical trauma unnecessarily. Given the degree of uncertainty, a cautious radiologist may seek a second opinion: how can the MammoGrid system support her? She may invoke a CADe service; the best among these can identify features which are not visible to the naked eye. Another possibility is to seek out similar images from the grid database of mammograms and examine the history to see what has happened in those other cases. However, since each mammogram is taken under different conditions, according to the judgement of a radiographer ('radiologic technician') it is not possible to compare them as they are. Fortunately, a service exists which standardizes and summarizes the images, provided certain parameters are available—the type of X-ray machine and its settings when the mammograms were taken. Perhaps at this particular moment the radiologist's workstation is already working at full capacity because of other imaging tasks, so it is necessary for the image to be transmitted to a different node for processing. Since our grid is distributed across Europe, it now matters whether the node which will perform the standardization is in the same country or not. Let us suppose that it is a different country. A conservative outcome is to ensure that, provided the regulatory conditions in the country of origin and in the country where the processing will take place are mutually compatible (i.e. logically consistent, capable of simultaneous satisfaction) that they are both complied with. If one set requires encryption, say, but the other does not, the data must be encrypted. If both sets of regulations allow the image to be transmitted unencrypted but one country requires all associated data transmitted with the image to be pseudonymised, this must be done. These are human decisions, but it is clear that they can be automated. Where will responsibility lie if something goes wrong in this process? In any case, the story has further ramifications: the whole idea of MammoGrid is to build up a rich enough database of images and case histories to provide a sound basis both for diagnostic comparison and for epidemiology. Once standardized and returned, is the image now to be stored and made available to others for comparative use, or is it to remain outside the system. This is now a question of informed consent. Will a service, in the sense we have already used the term, be trusted to determine whether such informed consent as the patient has given covers this question? There are, naturally, many more questions of a similar nature.

A further question arises in this context as to professional competencies in different countries. Imagine that a radiographer in one country, Italy say, is allowed to annotate an image (or to launch without medical supervision a CADe service to annotate an image) but then that mammogram with its annotation is used in another country, say the UK, by a radiologist to offer a second opinion, What should happen if in the UK a radiographer would not have had the 'professional competence' to annotate unsupervised? Is the radiologist at risk for having relied on an unauthorized annotation?

There is an almost invisible aspect of this initiative which deserves attention but will only be briefly touched on here. How is such a system to fit into the modern conception of evidence-based medicine, i.e. medicine that is based on scientific results? Evidence-based practice rests on three pillars: medical knowledge, as much as possible based on 'gold standard' (double-blind, controlled) clinical trials whose results have been peer reviewed and then published; knowledge of the patient, as complete as the record allows; and knowledge of the resources, procedures and protocols available in the setting where the encounter with the patient is taking place. However, the MammoGrid application we have described above plays a part in the 'dynamic' construction of knowledge. If images and histories are to be used as part of the diagnostic knowledge in new cases, it is imperative that they are collected with as much care and rigour as the cases in a controlled trial. Therefore, it is essential to know the 'provenance' of the data with precise details of how it has been handled (e.g. if standardized and subjected to CADe, which algorithms were used, set to what parameters, by whom, and if capture and interpretation were subject to appropriate practice standards). This set of issues has been labelled "the question of practice-based evidence for evidence-based practice". If this were to be accepted

as an appropriate source of diagnostic information, the underlying grid services, which maintain it, would have to make quality judgements without human intervention.

4.4. *The 'Whole Person' and genetic medicine*

A major breakthrough in healthcare is anticipated from the association of genetic data with medical knowledge. This would suggest that genetic information would have to be accessed routinely in the course of healthcare. Viewing this as part of the information held on a patient raises a number of difficult problems. Among these are the predictive value and the shared nature of genetic information. Knowing a person's genome could mean knowing what diseases they may or may not be susceptible to. Knowing one person's genetic map also reveals that of his or her siblings' in large measure. This introduces a range of questions, from confidentiality to 'duty of care' issues. If physicians will be held liable both for what they do and what they do not do, is it necessary for the underlying knowledge technology to 'be aware' and to inform them of the possibilities?

The grid could provide the infrastructure for a complete 'electronic health record' with opportunities to link both traditional patient data and genetic information to bring us closer to the ideal of genomic medicine.

4.5. *Health-e-Child project*

Among many questions being investigated in current projects is a set concerning development and illness in childhood, especially conditions in which genetic predisposition is at least suspected and in the diagnosis of which imaging is also essential. Physicians want to know how certain genes impact the development of diseases and radiologists want to know what the earliest imaging signs are that are indicative of a disease. For example, the Health-e-Child project [16] is investigating paediatric rheumatology, cardiac dysmorphology and childhood brain tumours using this approach. Consider its aims:

(i) To gain a comprehensive view of a child's health by vertically integrating biomedical data, information, and knowledge, that spans the entire spectrum from genetic to clinical to epidemiological.
(ii) To develop a biomedical information platform, supported by sophisticated and robust search, optimization, and matching techniques for heterogeneous information, empowered by the Grid.
(iii) To build enabling tools and services on top of the Health-e-Child platform, that will lead to innovative and better healthcare solutions in Europe:
    Integrated disease models exploiting all available information levels;
    Database-guided biomedical decision support systems provisioning novel clinical practices and personalized healthcare for children;
    Large-scale, cross-modality, and longitudinal information fusion and data mining for biomedical knowledge discovery.

With major companies looking to translate research results into products, successful outcomes from this and other projects would bring the scenario described above closer to reality.

A less obvious outcome from this research may be a reduction in the degree of invasive genetic mapping that may be necessary to address certain paediatric conditions. If a strong association is established between an imaging feature and a genetic mutation, it may then be used to limit the need for blanket genetic screening, restricting attention to those with the give imaging telltale or eliminating the need entirely. This would be a case where technology would at least indirectly contribute to reducing data protection issues, although the implicit conflict between duty of care and data protection remains (for example, in cases where findings may have implications for the health of siblings).

5. Conclusions

In light of the increasing use of technology in healthcare, and the likelihood of further significant use of technology in the future, it is important to take into account the ELSE. This paper has taken three levels of perspective: foundational principles, formalising principles in law, and an application domain in the context of the grid (representing a new technological context). Through this approach we have highlighted the ethical principles associated with healthcare practice and medical research (and, by extension, their rationale), how the law addresses issues pertinent to the medical profession in the digital domain, and how changes of context are relevant in the way they challenge existing cultural practice.

To fully exploit the benefits of developing technologies, and to facilitate the mutual understanding of the impacts of technology on ethical principles and consequent regulation and practice, there needs to be a mutual engagement and exchange between technology developers, ethicists, and above all, – in the light of issues raised in this article – the medical profession. Cross-disciplinary (and interdisciplinary) training would aid understanding. At a minimum, technologists need to be educated in the basics of ethical, legal and social considerations; these are issues they are apt to be unaware of at first, and to wish to ignore once aware of them, not for any malicious reason but because they are, or at least appear to be, an obstacle to technical development. On the other hand, ethicists, lawyers, journalists and politicians need to understand what the technology can do in a far more textured and nuanced manner than is common at present; this requires exposure to the culture of technology as well as to the basics of what current and foreseeable technologies can do. This discussions resulting from this paper is an opportunity to begin the exchange, and to open a dialogue aimed at reducing the gap between disciplinary cultures, different understandings, and divergent long-term aims and intermediate objectives.

Conflict of interest

None.

REFERENCES

[1] H. Muller, C. Lovis, A. Geissbuhler, The medGIFT project on medical image retrieval, in: Proceedings of First International Conference on Medical Imaging and Telemedicine (MIT 2005), August 16–19, Wuyi Mountain, China, 2005.

[2] T. Yoo, J. Ackerman, Medical image modeling tools and applications: open source software for medical image processing and visualization, Commun. ACM 48 (2) (2005) 55–59.

[3] W. Lowrance, Privacy and Health Research (1997). http://aspe.os.dhhs.gov/datacncl/PHR.htm.

[4] T.L. Beauchamp, J.F. Childress, Principles of Biomedical Ethics, 5th ed., Oxford University Press, NY, 2001.

[5] HEHIP, A Handbook of Ethics for Health Informatics Professionals, The British Computer Society, 2003 (endorsed by the International Medical Information Association).

[6] I.N. Bankman (Editor-in-Chief). Handbook of Medical Imaging Processing and Analysis, Academic Press, 2000.

[7] J. Moor, What is computer ethics? Metaphilosophy 16 (4) (1985) 266–275.

[8] J.G. Hodge, L. Gostin, P. Jacobson, Legal issues concerning Electronic Health Information, JAMA 282 (1999) 1466–1471.

[9] Department of Health: Confidentiality: NHS Code of Practice, November 2003. http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253.

[10] Health Which?: The Public View on Electronic Health Records, Health Which? and NHS National Programme for Information Technology, October 7, 2003: http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4055046.pdf.

[11] M. Ndeti, C.E. George, Pursuing electronic health: a UK Primary Health Care Perspective, in: M. Funabashi, A. Grzech (Eds.), Challenges of Expanding Internet: E-Commerce, E-Business, and E-Government: Proceedings of the 5th IFIP Conference on e-Commerce, e-Business, and e-Government (I3e'2005), Poznan, Poland, October 28–30, Springer, USA, 2005.

[12] The Information Commissioner's view of NHS Electronic Care Records, 2007. http://www.ico.gov.uk/upload/documents/library/data_protection/introductory/information_commissioners_view_of_nhs_electronic_care_reco%E2%80%A6.pdf.

[13] NHS: The Caldicott Guardian Manual, 2006. http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/policy/resources/new_guidance.

[14] Cancer Research UK factsheets for professionals, especially. Breast Cancer and Lung Cancer both available at: http://info.cancerresearchuk.org/ourpublications/healthprofessionals/factsheets/. See also female mortality data at: http://info.cancerresearchuk.org/cancerstats/mortality/females/ (all accessed 12.06.07).

[15] The Information Societies Technology Project: MammoGrid—A European Federated Mammogram Database Implemented on a Grid Infrastructure, EU Contract IST-2001-37614, 2001.

[16] The Information Societies Technology Integrated Project: Health-e-Child—An Integrated Platform for European Paediatrics Based on a Grid-enabled Network of Leading Clinical Centres, EU Contract Number IST-2005-027749, 2005.