



A moral approach to electronic patient records

N. B. FAIRWEATHER and S. ROGERSON

Centre for Computing and Social Responsibility, Faculty of Computing Sciences and Engineering, De Montfort University, The Gateway, Leicester, LE1 9BH, UK; e-mail: ccsr@dmu.ac.uk

Abstract. This paper seeks to establish a morally appropriate balance between the various moral standards that are in tension in the field of Electronic Patient Records (EPRs). EPRs can facilitate doctorpatient relationships, however at the same time they can undermine trust and so harm the doctorpatient relationship. Patients are becoming increasingly reluctant to tell their own doctor everything that is relevant. A number of moral principles and the question of consent to release of records are considered here. There is also explicit mention of the principles for the treatment of the EPRs of the dead. A number of tensions between principles are explored, including that between privacy and promotion of welfare, both in an emergency and in more routine situations. The discussion also includes the tension between access and the right to not know about a condition that may undermine, for example, self-esteem; and the tensions between principles that arise when epidemiology, public health surveillance and healthcare evaluation are conducted. Suggestions are made about an appropriate balance between the principles. It is suggested that the patient's right to informed consent should be dominant.

Keywords: *Electronic patient records; Health informatics; Medical ethics; Privacy; Medical data access*

1. Context

Healthcare computing (also called medical informatics) is one of the fastest growing areas of information and communication technology (ICT) application. ICTs have been applied in healthcare to performance indicators, financial (including insurance) systems, paramedical support, emergency services, electronic patient records, computer aided diagnosis, clinical governance, remote surgery, research support and hospital management. The implementation of information systems in healthcare is inevitably ethically charged and moving at a faster pace than ethical consideration of those developments. Developments in the exchange of electronic patient records are a particularly strong theme in the implementation of information systems in healthcare. Thus, in the United Kingdom, NHSnet, a national health information network has been established for some years (p. 307) [1], yet adequate security infrastructures for it are *still* some way off [2; see also (pp. 6–9) 3].

All uses of ICT in healthcare should ideally promote, and must certainly not conflict with, the fundamental principles of medical ethics. There is a widespread consensus around the principles of beneficence, nonmaleficence, and respect for patient autonomy within medical ethics, and substantial acceptance of the principle of distributive justice (p. 38) [4]. Beneficence can be taken as meaning a duty to promote good and to act in the best interest of the patient

and the health of society.[†] Nonmaleficence indicates a duty to do no harm to patients. Respect for patient autonomy can be interpreted as a duty to protect and foster a patient's free, uncoerced choices. Finally, distributive justice implies ensuring that the costs and benefits of healthcare are fairly distributed, and according to some theories ensuring that the relationship between the distribution of costs and benefits is fair.

At a philosophical level, certain of the principles are more closely associated with particular positions in general ethics: thus autonomy might be associated with deontologism and beneficence with consequentialism. Such an association is, however, simplistic. As Beauchamp and Childress (p. 110) [4] say, 'Many different theories lead to similar action-guides and . . . It is possible from several of these standpoints to defend roughly the same principles, obligations, rights, responsibilities, and virtues'. Many plausible consequentialist theories, for example, would give rise to a deep concern for autonomy.

Whatever the level of agreement about these principles of medical ethics, there may at times be a tension between the duties implied by these various principles; and between them and other principles, either derived from them, or with other strong moral support. It may appear inadequate to start from a basis of principles that at times are in tension, but since no claim to have identified the perfect moral theory has even come close to having been proven, there is, in our opinion, no better starting point available, and the questions at hand are too urgent to wait for a convincing proof of the perfect ethical theory to be discovered.

While this paper is interested in principles, it is not attempting to develop the perfect principles no matter how impractical; our position, rather, is that practicality is one factor that needs to be considered, along with principles, perhaps through 'The method of wide reflective equilibrium' (p. 449) [5], after Rawls and Griffin).

This paper considers one aspect of healthcare computing, electronic patient records (EPRs). It identifies a viable moral approach to EPRs taking into account the ethical principals discussed. EPRs enable some or all of the medical history of patients to be computerized. They offer new methods of storing, duplicating, manipulating and communicating medical and non-medical information of all kinds, including text, images, and recordings of sound, video and tactile senses (p. 4) [6], (p. 2) [7]. Thus they can be more powerful and flexible than paper-based systems. They allow providers, payers and patients to interact more efficiently, and in ways that improve health and can be life enhancing. Perhaps for these reasons, governments appear to favour national healthcare infrastructures with 'longitudinal' patient records, which cover a patient's complete medical history [8] from the womb (or perhaps even before conception) to the grave.

2. Inappropriate balances

The centrality of trust to the doctorpatient relationship can to some extent be gauged by the fact that ensuring patients will find medical professionals trustworthy provides a substantial part of the reasoning for regulation of medical

[†]It should be recognized that 'promoting good', 'acting in the best interest of the patient' and 'acting in the best interest of the health of society' give beneficence different senses in different contexts.

professions (p. 7) [4]. EPRs can facilitate doctor–patient relationships through the use of computerized notes, which the doctor and the patient can share and contribute to. However, at the same time EPRs can harm the doctor–patient relationship and undermine trust. For example, in the US, medical data clearinghouses sell patient data to a range of organizations including insurance companies, police departments, employers and drug companies (p. 91) [9]. In doing so they have the potential to reduce the cost of healthcare, and thus support the beneficent aim of medicine.[†] However, the knowledge that data may be widely distributed and sold means that patients are becoming increasingly reluctant to tell their own doctors everything about their symptoms and the possible causes of them (p. 89) [9, 10], (p. 6) [7].

The potential for severe damage to the relationship between doctors and patients if privacy is not adequately protected has been well known for some time (see, for example, (p. 177) [11], (p. 78) [12]). The relationship depends heavily on confidentiality, and patients withholding information about their symptoms and possible causes of them can damage the quality, and hence (paradoxically) the efficiency of care.

There has not been enough work on defining ethically appropriate procedures and criteria for disclosures to the vast array of potential secondary users of health data such as managed care evaluators, insurance companies, and drug companies. The locations of the boundaries of morally legitimate trade in medical information have not been sufficiently explored. More work is also needed on ensuring that data is completely anonymized when traded, even where patients have rare medical conditions and other unusual attributes (perhaps unusually high levels of educational qualification) that make them easy to identify when these facts are combined (see (pp. 2, 7) [13]). The aim of this paper is to stimulate further debate about EPRs and to encourage others to participate in this essential work.

3. Other research into the problem

The single most important answer to the problem that has been produced hitherto by other researchers is the Opinion of the European Group on Ethics *Ethical Issues of Healthcare in the Information Society* [6], which like this paper, ‘confines itself to the ethical [considerations] of the use of person identifiable personal health data’ (p. 3) [6], (emphasis removed). The ‘Opinion’ identified a number of relevant ‘value conflicts in the provision of healthcare’ including ‘effectiveness versus confidentiality’, ‘privacy versus the collective good’ and ‘efficiency versus beneficence’ (p. 9) [6].

Since that ‘Opinion’, further (less comprehensive) research has been published [7], [14, 15, 16], providing further insights that have been taken into account in this paper. Alpert [9] has made another substantial contribution on these issues. However, Alpert concentrates on the tension between privacy and needs to ‘maximize appropriate access to personal information’ (p. 75), and in doing so reaches solutions that do not give enough weight to the influence of other moral principles.

The contribution of this paper differs from previous work by taking an interdisciplinary approach with insights from information systems and from

[†]Potentially in either the individual or social senses of the principle of beneficence, depending how health care is paid for.

moral philosophy, and by taking on board a wider range of sources, including material that has become available since previous work in this fast-moving field. It identifies and considers a larger number of relevant tensions between moral standards than previous work, but unlike Wagner *et al.* (p. 10) [6] is not committed to the view that ‘Trust is a fundamental ethical value in itself’, rather seeing strong grounding for trust in other, more fundamental, values. We further believe calls for closed networks that restrict access whilst operating globally (p. 11) [6] to be unsustainable. The failure of the ‘Opinion’ of Wagner *et al.* to explicitly recognize the problems that can be caused by doctor–patient records being inappropriately widely available is an especially serious shortcoming that this paper seeks to rectify.

4. Principles

As already stated, three of the most widely accepted principles of medical ethics are beneficence, nonmaleficence, and respect for patient autonomy. Thus there is a fiduciary responsibility on doctors towards patients ‘of acting only in the patient’s best interests’ (p. 79) [12] which implies a duty normally to keep medical records private, as would be required by the Hippocratic oath, where it is still taken.

Others have argued that ‘Electronically based patient records . . . , are . . . patient analogues’ (p. 105) [17], and because of this the promotion of autonomy requires allowing control for the patient over their analogue. We are not entirely convinced by this argument. Patients certainly have an interest[†] in what happens to their records after they are dead; yet their autonomy cannot be promoted once they are dead, even if their ‘analogue’ persists as if they were alive. Concern for privacy derived from the promotion of autonomy as applied to a patient analogue appears to be too limited in scope.

Breaches of the duty of confidentiality can leave doctors subject to being disciplined by their professional body, and prosecution in many legal systems (p. 7) [16]. The fiduciary relationship extends to health information professionals (p. 105) [17] and thus, ‘The health care informatician should respect the privacy of individuals, groups or organizations and should know that any breach of their privacy through the utilization of their data without their authorization or consent constitutes a considerable threat to their person’ (p. 384) [18]. The principle that consent must be properly informed is well established in medical ethics (pp. 142–157) [4]. However, this is not enough, because it must be remembered that there are times when individuals are required to give ‘consent’ on pain of being excluded from significant benefits. It may even be that continued employment may on occasion be effectively dependent on giving such ‘consent’ [19], although it is more common for such benefits as gaining employment or securing life insurance to be conditional on releasing medical data in some jurisdictions. A requirement that access to private information be with ‘consent’ would not be enough on its own to ensure that such access is morally correct.

Further, there are times when it is morally appropriate for access to be given without consent having been obtained from the data subject. These

[†]At minimum an anticipatory interest while they are still alive: we will not explore here the question of whether the dead still have interests.

circumstances may arise when the patient is unconscious and cannot give permission, or when there is an overriding public interest (such as to prevent the spread of a communicable disease by tracing carriers; see also (p. 8) [16]). When consent cannot be obtained from the data subject, access should only be with the consent 'of a duly empowered legal authority acting with due process of the law' (p. 336) [20]. This requirement for legal sanction is, like 'consent', not enough on its own. In a regime that is corrupt, arbitrary, liable to prejudiced discrimination, totalitarian or otherwise acting beyond its moral authority; legal sanction may be given in circumstances where it should not, or denied when it should be given.

Privacy is not an all-or-nothing concept. A person never has either complete privacy (even the sole inhabitant of an abundantly fertile island will feel the impact of global climate change, which has been caused by other people), nor utter lack of privacy (even in the most humiliating imprisonment, some of the prisoner's thoughts remain private). Privacy can, as with those two extremes, relate either to the ability of others to make an impact on your life ('associative privacy': [21]), or to knowledge about you ('informational privacy': (p. 340) [22]). Very often, but not always, both types of privacy are closely intertwined in practice (knowledge about my life would enable you to have impacts on it, while many of the impacts that you can make on my life leave you with the knowledge that my life has been affected in that way). This paper is more centrally concerned with privacy regarding knowledge about the subject.

The degree of privacy could, in principle, be different for each piece of knowledge about a person (insofar as it makes sense to talk in terms of discrete pieces of knowledge). For each piece of knowledge about an individual, *x*, the degree of privacy would be determined by how many, and which, other individuals and organizations had access to the knowledge at what effective cost ('cost' here should not be thought of solely in financial terms, but also in terms of time and effort, the risk of effective sanctions, whether from the law or others, etc.). Thus for each piece of knowledge, greatest privacy is achieved when nobody but you knows it, and no amount of resources (not even use of extensive torture facilities) could cause it to be revealed. Similarly, for each piece of knowledge, zero privacy would be when everybody who will ever live knows that about you: thus zero privacy is not achievable in respect to any single item of knowledge, although near-zero privacy in respect of some items of knowledge is possible for such world famous people as the late Diana, Princess of Wales.

According to Nevado LLandres (p. 76) [12], it is 'quite clear to everyone that under no circumstances should the use of databases diminish the right of the patient to the privacy and confidentiality of his data'. However, the use of databases is diminishing the practical extent of privacy and confidentiality. It may be that the *right* has not been diminished, but evidence suggests that the extent of *respect* of the right is declining. Violations of medical privacy may be easier than ever before because of the very efficiency of computerized systems, so that we are now in an age when 'Neither physicians nor patients can assume that rules regulating the use of patient information will effectively stop potential breaches of confidentiality' [19]. The extent and severity of damage to the privacy and broader well-being of a patient [23] whose confidentiality is violated may be proportionately greater because of the amount of data held within an

EPR and the ease with which it can be replicated, distributed and data-matched.

Consideration of the principle of beneficence suggests that the best interests of patients are served (1) by improvements in care at reasonable and affordable cost; (2) by reductions in cost resulting in more care being provided for the same expenditure; and (3) by reductions in cost enabling the same care to be provided for less cost, freeing up resources to promote patient welfare in other fields.

Gritzalis *et al.* argue (p. 385) [18] that ‘The user of a medical computer system will not design systems that can come to originate considerable harm to the health of the patient or the reputation of the health care professional’. However, the *potential* for considerable harm is virtually inevitable with medical computer systems, because even the best-designed system meeting all appropriate standards for safety-critical systems is liable to have the potential for being a contributory factor in considerable harm when in the hands of someone evil and technically proficient.

Distributive justice also plays an important role in medical ethics, and requires that the various outputs of healthcare (including medical well being), and the costs to achieve them, be fairly distributed.

4.1. *The fair information principles*

According to Kluge (p. 336) [20], there has been ‘a remarkable convergence’ in regulation of medical informatics ‘towards a uniform position centred in the so-called “fair information principles”’. These principles are, in brief: openness, limitation of collection, limitation of disclosure, limitation of use, security and access (see also (p. 90) [24] where these principles are re-worked into a more coherent, but less widely accepted, list of seven principles). Each of these is considered in turn.

- **Openness** is strongly associated with respect for patient autonomy, as without knowledge of ‘the existence of an electronic data-bank’ or ‘the kind of information it contains’ (p. 336) [20] it is simply impossible for the patient to make autonomous decisions on relevant questions (which may include whether to seek medical attention for an injury sustained in a particularly embarrassing way, for example). Respect for patient autonomy requires that patients be educated about the nature of EPRs and their rights (p. 13) [6], and be able to effectively articulate their views.
- The principle of ‘**limitation of collection**’ is an aspect of the more general requirement to respect privacy, requiring that data only be collected and held if they are ‘necessary to achieve the legitimate aims’ of the information system, and have been collected using ‘ethically defensible’ procedures (p. 336) [20].
- ‘**Limitation of disclosure**’ is essentially another way of expressing the privacy questions relating to consent for disclosure of data as discussed previously.
- ‘**Limitation of use**’ relates to considerations both of privacy and autonomy, this time requiring that the uses to which data are put are limited to those which are ‘duly empowered legitimate purposes’ of the information system (p. 336) [20]. Clearly, any restriction on the extent of distribution and use of information about individuals promotes privacy. Autonomy is promoted by limitations of use, because they enable the data subject (the patient, for medical data) to give (or decline to give) consent to the purposes to which the data actually will be put.

- **Security** is essential to privacy in practice. In a world in which a significant proportion of people seek information to which they are not entitled,[†] the only way to make sure that an item of knowledge is available to a limited number of people and organizations is to employ data security systems. These systems must be capable of withstanding sophisticated (and simple) attacks by those seeking to breach the security, since there have been successful attempts to breach security of EPR systems in the past (p. 11) [16].
- **'Access'**, as a 'fair information principle' is concerned with the right of the *data subject* to gain access to the data about them, and to correct it if it is inaccurate, incomplete, or contains irrelevant material (p. 336) [20]. The Shipman murder case in the UK, however, suggests that correction of records should not be technically possible without the agreement of two doctors. Access to data about himself or herself would enable an individual to ensure that beneficence were maintained, at least in their respect as an individual (see also below on how 'access' may at times be in tension with beneficence).

Kluge argues (pp. 338–339) [20] that EPRs are an analogue of the patient in a kind of nominal decision-space and as such should be treated according to ethical standards that mirror the standards that apply to treatment of the physical patient. In this light Kluge argues (p. 340) [20] that the 'fair information principles' are 'Not the ultimate justification of an ethical course of action, but a heuristic move that is adopted for the sake of inferential brevity', when the right course of action is more correctly inferred from more basic moral principles. It is also clear, as Kluge points out (p. 340) [20] that, for all their usefulness, there are circumstances in which the right course of action may run counter to the 'fair information principles'.

4.2. *The dead*

There has been remarkably little consideration of moral obligations with respect to the dead [26], but the issue is in practice inescapable when considering electronic patient records: a high proportion of the entries on an EPR are likely to relate to the period immediately before death.

In the only legal system with which we are sufficiently familiar (the English), the dead have no right to have their good name protected from defamation. It may be said that the dead no longer have rights, because they can no longer make claims, when 'the content of a system of rights is historically conditioned by the making of claims' (p. 64) [27]. However, we are interested in morality, not the law, when not all morality is rights-based; not all rights are claim-rights [28]; and 'there is a distinction to be made between *having* claims and *making* claims. The mere fact that someone claims something is not sufficient to establish it as his right' while 'someone may have a claim relative to me whether or not he makes the claim or is even able to make a claim'. (p. 64) [27].

It may be argued that the dead 'are no longer morally significant persons', and thus the only basis for respect towards the dead is the 'psychological harm to the living relatives' [29]. While we are not convinced that this is the only basis, this basis alone could give rise to substantial obligations with respect to the

[†]In a recent survey, over 30% of the respondents agreed, or strongly agreed that "It is acceptable for me to use other employees' access codes with their permission to access data normally hidden from me" (pp. 28–29) [25].

treatment of the dead. People do like to think well of the dead, and could be anxious, for example, that some aspects of a patient record remained confidential, rather than be allowed to tarnish a reputation.

Most of us do care about what happens to our body and our reputation after our death. This suggests that how we treat the dead may be morally important independent of the effect on relatives, at the very least because those who are alive are anxious not to be treated the same way. It is also worth remembering that the relationship of medicine to the dead is decidedly ambiguous: much medical knowledge (especially anatomy) has been derived from treatment of corpses which in other contexts would be clearly unacceptable, while at times medicine appears to be working flat-out to prevent death at all costs.

Furthermore, the EPRs of the dead, like EPRs of the living, can have direct relevance to knowledge about the medical status of other family members. This gives rise to particular problems, however, with the dead, which are considered below.

5. Tensions between and within principles

In practice there can be a need to provide timely access to as much relevant data as possible to allow the correct treatment of a patient, and especially in an emergency. ‘An accurate medical record helps the health care team avoid unintended complications by alerting them to a patient’s condition and current treatment ... [therapeutic] drugs ... carry the risk of significant side effects and may interact negatively with other medications.’ [19] Electronic patient records can facilitate such timely access as is needed, but in an emergency access to the EPR may be needed (p. 7) [16], possibly even by a paramedic who does not have ‘full’ medical training, or by a doctor acting outside their field of medicine. Even more difficult cases arise when the only timely treatment available would be given by somebody who is not employed in any of the medical or related professions, and not subject to the associated enforcement of professional standards, but rather has received brief training in emergency life support. This need for access could apply when the patient has never met the person accessing his/her EPR, when the patient is unconscious and next of kin cannot be contacted sufficiently quickly. How can sufficient access to data be provided to such people without access to the EPR being open to all?

Although there is a need to provide timely access to as much relevant data as possible, patients should have the ability to allow selective access to their records. For example a woman who has had an abortion may visit a doctor for treatment of an ailment that cannot possibly be related: she should have the right to withhold from the doctor such especially sensitive information that is not relevant to the matter at hand [30]; contra (p. 10) [6]. There are, of course, practical difficulties attached to patients making judgements about whether aspects of their history are relevant. However, EPRs can provide a greater potential for patient control in these matters, because a computer program can assess the likely relevance given other inputs (for example of current symptoms) before it even suggests to the patient that revealing a particular item of data may be beneficial.

The ‘fair information principle’ of ‘access’, while often being a useful way of maintaining beneficence (see above), can at times be in tension with other

aspects of beneficence. Patients should also have the right to *not* be informed of some medical facts where, for example the fact may undermine self-esteem and the way in which they live their lives (such as genetic data or information about terminal illness).[†] Where genetic data or data about infectious diseases is present that may be undermining in this way, family members also have the right to *not* be informed in the same way. While normally this would not be a problem (as EPRs are personally confidential among adults), there is particular cause for concern with the EPRs of minor children. Another possible cause for concern would be if relatives were to be allowed control of the EPRs of the deceased. It is appropriate for somebody to be appointed to uphold the interests of the deceased with respect to their EPRs. This cannot, however, normally be a relative of the deceased, because if it were, an exception would have to be made whenever the record contained data that could also be undermining to the family member. If such a procedure were followed, the making of such an exception would be tantamount to acknowledging the existence of the very data from which it was intended to protect the family member. A different procedure, outlined below, is needed.

There are further difficulties with genetic data and data about infectious diseases that are likely to be passed between family members. There is a mismatch between *individual* control over the collection and storage of EPRs and *individual* access to EPRs (on the one hand), and information that applies to a group of family members (on the other) (p. 1) [14]. One often cannot prevent such information about oneself being gathered, stored, or accessed as part of a family member's EPR. Worse, 'in some cases', such as where a genetic condition only affects one gender, 'the information has greater significance for others than it has for the one from whom it was gathered' (p. 2) [14].

Electronic access to patient data can also be beneficial in a variety of settings where inaccurate interpretation of hand-written messages can have harmful effects. For example, electronic transmission of prescriptions with digital signatures can prevent some cases of potentially dangerous incorrect dispensing.

It is not in any way a matter of controversy that 'notations of a psychiatric illness carry the risk of potential discrimination that could destroy the patient's current and future employment if the information is insufficiently protected' [19]. It would not, equally, be a matter of dispute that medical notes relating to a number of other types of symptoms or hinting at a number of other types of illness or medical procedures could cause similar harm if revealed to current or prospective employers. While this problem has not been entirely created by digitization of patient records, the increases in ease of duplication, manipulation and communication of records that digitization has enabled; make disclosure of more information and to more people than ever before very real prospects. The prospect of unauthorized access to records has also been increased by digitization.

Epidemiology, public health surveillance, and healthcare evaluation, each seek to promote the health of society. In the era of ICTs each encourages the collation

[†]This right may appear paradoxical, in that if rights were only exercised at the request of the right-holder, this right could never be successfully exercised. However, as stated above, having such a claim does not require an individual to be in a position to actually make such a claim: a right can exist even if no individual is ever in a position to decide whether to exercise it. It is worth noting that beyond having a right to not be informed, *R v Mid Glamorgan Family Health Services Authority and another, ex parte Martin* [31] holds that a patient does not have the right to access to medical records under such circumstances.

and comparison of many disparate facts about as large a proportion of the relevant population as practical (while the limits of the relevant population may not always be easy to discern, encouraging a wide interpretation). The databases so generated can be used, for example, ‘to trace long-term effects of certain drugs, trajectories of particular diseases, [and] outcomes of particular medical interventions’ (p. 5) [6]. They could also detect unusually high death rates, detecting some multiple murders (as in the Shipman murders), and flawed practice (as with the Bristol babies case in the UK). The large databases so used can give rise to a tension between the privacy of some individuals and the health of another group which may, or may not, overlap the group whose privacy is at stake. Clearly, principles relating to distributive justice are at stake here. There is also the possibility that data collected for epidemiological or scientific research might provide information relevant to the potential treatment of an individual, giving rise to a tension between the health of an individual and their own privacy (p. 231) [32].

Due to considerations such as the principle of beneficence,[†] in healthcare there is a need to cut costs that are not inevitable costs of treatment where this can be done without harming treatment. Electronic transfer of patient records offers the potential to save money when compared to traditional methods (p. 308) [1], freeing resources for ‘front-line’ patient care. As all security and privacy technologies come with associated costs, there is a direct tension here between privacy and financial goals.

The categorization and profiling of patients by managed care evaluators, insurance companies and the like also has the potential to enable cost savings, but may enable discriminatory or exclusionary effects that can run counter to the principle of nonmaleficence for some, even while promoting beneficence for others.[‡] Thus principles of distributive justice could be violated at the same time as the principle of nonmaleficence.

It should be apparent that ‘the user of medical software assumes the social responsibility of utilizing it to promote the quality of the health care provided to the patient and the moral obligation to question whether or not its use is beneficial to the patient’ (p. 384) [18]. However, such concerns of immediate benefit to particular patients might be in tension with the potential benefits to other patients of more comprehensive testing, etc. The issues here are exactly the same as more typical medical trials.

6. Striking a balance

It is clear that a balance must be struck so that EPRs might realize their potential beneficial status, whilst ensuring the risk of harm is minimized. The main elements of this balance are discussed in this section. Further research may in due course disturb the current reflective equilibrium between the various principles which are in tension and between the principles and questions of practicality.

A patient’s right to informed consent should be dominant, and in order to enable this, education about these issues should be available to patients (cf (pp. 10, 13) [6]). All patients should, following the ‘fair information principle’ of

[†]In the social sense, and in the individual sense if there is individual payment for treatment.

[‡]In the individual sense of the principle of beneficence, and in the social sense if the categorization is widespread.

openness (p. 336) [20], have practical access to information about the existence of all databases with medically relevant information about themselves. There are rare exceptions. The first exception is where the knowledge about the very presence of a record in a particular database itself (regardless of content) may undermine self-esteem and the way in which the patient lives their life.[†] The second exception is when knowledge about the existence of a record in a database may seriously jeopardize the health of others, seriously jeopardize an investigation into a serious crime, or have a similar impact.

A patient should have effective control over his/her data and the ability to prevent any casual distribution that might be harmful to himself or herself, ensuring EPRs maintain nonmaleficence.[‡] There may need to be exceptions again, for example to combat contagion, but where the patient has at least an ordinary degree of rationality, strenuous efforts should be made at persuasion before release of the information is taken out of the individual's control.[§] Where a patient does not have the degree of rationality routinely present among adults, his/her representative (parent or guardian in the case of a young child) should have the control that the patient would normally have. We agree with Barroso (p. 4) [16], and certain jurisdictions, that 'If a child is regarded as mature enough to make conscious decisions in relation to the confidentiality of personal information, the law should ... recognize this and the child should have the right to make the decision'.

Upon death, the executors of the estate should be able to exert control over the dead person's EPR [33], except when the executors are family members, in which case a special 'patient record executor' should be appointed in all cases: it should thus be standard practice for wills to appoint a 'patient record executor' at the same time as the will is written if the executors are family members. The patient record executor (whether the same person as the general executor or not) should have most of the rights over the records that the deceased would have had (without any restrictions that may have been in place over records knowledge of which might have harmed the, now deceased, patient). Given that most patients never express any opinion about their records, and that when opinions are expressed, they are usually concern for privacy or about 'consent' to release records, it is not anticipated that the patient record executor would be called upon in any but the most exceptional cases. Further consideration is needed on whether they should have the right to correct records. On the one hand an incorrect record can no longer harm the patient's health, and the possibility of introducing inaccuracies is much greater than when the patient can be consulted.[¶] On the other hand, inaccurate data concerning the dead might harm living family members. Individualization of data (see below) may ease this tension somewhat.

[†] It is recognized that this exception could allow authorities with ill will to ignore the principle: there needs to be protection to ensure that this exception genuinely only applies when stated. Further, it may be worthwhile for there to be a procedure for routinely asking *all* citizens what their attitude would be to knowledge of such sorts, and for recording such attitudes in advance of them becoming relevant.

[‡] In the case where a patient does not know of the existence of data, due to the considerations in the preceding paragraph, the restrictions on the distribution of such data should be at least as strong as those on data that the patient does know about.

[§] We will leave to one side the operational details of what would constitute sufficiently strenuous efforts, since this paper is not about operational details.

[¶] Further information might possibly be added as a result of a post-mortem, or as further knowledge is gained through other sources.

Given the existence in EPRs of genetic data and data about infectious diseases that also apply to other family members, we suggest that information gathered should be ‘as individualized as possible (e.g. not recording [the identity of] siblings, parents, offspring)’ (p. 4) [14]. This will, however, reduce the amount of benefit that can be gained from some instances of genetic testing (thus inhibiting beneficence[†] to some extent). We have not, as yet, resolved all of the questions of how to reconcile this with the need to prevent the spread of infectious disease.

Where epidemiological data is required (including kinds that cannot be individualized while still maintaining their epidemiological relevance), anonymized data collection should be employed, employing suitable encryption and an anonymizing gatekeeper [15].

There needs to be safeguards to ensure that declining to give consent to access records (in employment and insurance contexts for instance) does not harm the patient unduly. This will have serious implications for employers who have been accustomed to health screening that enables them to decline to employ the disabled; and for insurers who have hitherto given cheaper or more comprehensive cover to those with a ‘clean bill of health’.

Patients should have the ability to allow selective access to their records, being assisted to make informed choices about when it may be appropriate to reveal information they would normally prefer to remain confidential.

The appropriate scope for EPRs, and patients’ rights with respect to their own medical information should be clearly defined. Prohibitions on certain sorts of uses of data and what principles should govern legitimate access to and use of personal health and medical data and information also need to be clearly enunciated in a way that ensures they are respected. In societies such as those that presently exist in the industrialized world, legislation is likely to be the most appropriate mechanism for such definition and enunciation. In societies where property is a dominant concern for the law, clarification of the ownership of patient data is vital. Mechanisms for the enforcement of applicable laws and oversight of use and access must be in place, adequately resourced and effective.

Harm to the doctor/patient relationship should not be taken lightly. While doctors have on occasion exaggerated the intimacy of the doctor/patient relationship; it is normally advantageous for such intimacy to be promoted,[‡] if patients are to be appropriately treated. Healthcare providers and funders and other potential recipients of medical data should understand the impact of receipt of data on the doctor/patient relationship (cf (p. 13) [6]), and be aware that the knowledge that data is being collected may bias the data in ways that dramatically reduce its value.[§] Against this background, recipients of data should ensure (1) that whenever possible data is only collected in ways that are not individually identifiable (including by combining with other data sets); (2) that the data collected is the absolute minimum required for the purposes at hand, which are themselves morally scrupulous; and (3) that the advantages of use and

[†]In the social sense, and in the individual sense for as yet unidentified individuals.

[‡]Although not by a reduction in the inhibitions and knowledge of the patient.

[§]Both by inhibiting patients from revealing symptoms and other medically relevant information, and by inducing doctors to avoid recording, or disguise the recording, of especially sensitive information. Such biases would render any subsequent statistical analysis of the data unreliable in unpredictable ways.

further distribution of data are weighed against the potential for harm to individuals and to the data stream of such use.

7. Implementation

While this paper does not focus on implementation, it must be explicitly recognized that there are serious issues in the implementation of Electronic Patient Records. These are briefly discussed in this section.

The movement of EPRs over the Internet, intranets and extranets raises particular concerns. The further (in terms of logical steps rather than physical distance) data is from its original source, the greater the risks of duplication, falsification, inaccuracy, manipulation and unauthorized distribution. There has been little effective control over data use over computer networks, with high levels of security for dial-in and Internet links. While encryption of data in transmission, and in storage, can ease these problems [34] (cf (p. 11) [6]) it is logically impossible for it to solve them: to be interpreted, data must be decrypted, yet 'passwords are considered by many to be awkward and unnecessary' and 'Re-establishing network connections can take so long that busy clinical staff avoid logging off between transactions' (p. 6) [3]. Another problem is that inappropriate 'insider access to medical records' has led to violations of privacy for some years [19]. While it may be possible to foster a good security culture, the first step is to recognize that purely technical 'solutions' are insufficient.

There should be clearly defined limits of access for each type of authorized person. When implemented, systems should provide security alarms linked to all functions that involve an element of browsing, copying or reporting [34], and record who has accessed sensitive information [19; (p. 3) 35].

While other issues are mentioned below, it is important to remember that manipulation, use or abuse of healthcare information is not needed to cause harm. The mere suspicion that information might be, or might have been, leaked can cause harm [19] (cf [8]) whether by inhibiting the doctor/patient relationship or by meaning that records are incomplete.

Another issue is accuracy of the original data. Health care workers 'may be highly capable and competent, but if they lack the training necessary to use the program correctly, they may cause irreparable harm; [thus] the ideal we seek is that the user introduce clinically accurate data into the computer' (pp. 76) [12]. However, that ideal may well not be achieved, with the potential for serious detriment to the health and wider well being of the patient.

7.1. Inaccurate data

According to Nevado LLandres (pp. 77) [12] 'if ... erroneous or inadequate symptoms were introduced [ie input], then the responsible party is the physician'. However, this leaves substantial problems. A requirement to guarantee adequate input of symptoms could lead to doctors conducting unnecessary duplicate tests with direct adverse consequences to patient welfare, and consequences through unnecessary expenditure. Further, it is quite possible for electronic patient records to be altered by someone (for example a technician) who is not medically qualified: responsibility thus cannot fall entirely on medical professionals. Worse, it is possible for an inaccurate record to persist long after the person who was morally responsible for the introduction of the

inaccuracy has ceased to practice: indeed, such inaccuracies could remain relevant to the (mis-)treatment of a patient long after the culpable person has died. While this was possible with paper records, the greater willingness to trust information that arrives in electronic form, the greater durability, the ease of reproduction, the ease of searching, and the greater distribution offered by electronic records all exacerbate the problem.

Another particular problem arises when there are suspicions about the privacy of the patient record. 'Failure to record significant diagnoses and therapies . . . puts patients at risk.' [19], yet because of the fear that patients may be harmed if records do not remain private, 'the practice of keeping 'double' records for patients [with psychiatric diagnoses] . . . has become widespread. Alternatively some clinicians . . . have created 'code language' to obscure the true content of clinical interactions' from those who were not present in the consulting room [19]. While there may be legal protection of the privacy of the patient record in many jurisdictions, such protections are not sufficient if there are still suspicions on the part of either the patient or their doctor that records will not remain sufficiently private for a long time. In both the USA and the UK, such suspicions would currently be well founded.

8. Conclusions

This paper has focused on the ethical issues surrounding the growing existence and use of electronic patient records. The tensions between conflicting needs have been discussed. A morally defensible approach to EPRs has been suggested which can be summarized as follows:

- A patient's right to informed consent should be dominant: thus education about these issues should be available to patients, along with information about the existence of all databases with medically relevant information about the patient (with some minor exceptions).
- A patient should normally have effective control over his/her data and the ability to prevent any casual distribution that might be harmful, ensuring EPRs maintain nonmaleficence. There need to be safeguards to ensure that declining to give consent to access records does not harm the patient unduly.
- Patients should have the ability to allow selective access to their records.
- The EPRs of the dead should be treated with the same consideration as those of the living.
- In contemporary industrialized societies, legislation should clearly define the appropriate scope for EPRs, and ownership of patient data. It should clarify what principles should govern legitimate access to and use of personal health and medical data and information, and patients' rights with respect to their own medical information. There should be prohibitions on certain sorts of uses of data. Mechanisms for the adequate enforcement of applicable laws and oversight of use and access must be in place.
- Healthcare providers and funders and other potential recipients of medical data should understand the range of impacts of all sorts of medical data sharing, including on the requirement for openness in the doctor-patient relationship (both if patients are to be appropriately treated and if accurate data is to be collected) (cf (p. 13) [6]).

EPRs are indicative of a society that is increasingly dependent upon ICTs. The impact of this morally sensitive application of ICTs cannot and should not be ignored. We urge those involved in the creation, use and promotion of EPRs to consider our suggestions.

References

1. POULOU DI, A. and WHITLEY, E. A., 1996, Privacy of Electronic Medical Records: understanding conflicting concerns in an interorganizational system. In *ETHICOMP96: III International Conference Values and Social Responsibilities of the Computer Science: Proceedings*, Volume 1, edited by P. Barroso Asenjo, T. W. Bynum, S. Rogerson, and L. Joyanes, (Madrid, Spain: Pontifical University of Salamanca in Madrid), 307–327.
2. SCHNEIDER, P., 1998 Europeans ready for privacy law. In *Healthcare Informatics* June 1998, 137–138. Online at http://www.healthcare-informatics.com/issues/1998/06_98/interntl.htm, accessed 09 March 1999.
3. GAUNT, P. N., 2000, Practical approaches to creating a security culture. Paper at *The 8th Working Conference of the IMIA WG4: Security of the Distributed Electronic Patient Record (EPR)*, Victoria, BC, Canada, 21–24 June 2000.
4. BEAUCHAMP, T. and CHILDRESS, J., 1994, *Principles of biomedical ethics*, fourth edition, (New York, USA: Oxford University Press).
5. HOVEN, VAN DEN, J., 1996, Computer Ethics and Moral Methodology. In *ETHICOMP96: III International Conference Values and Social Responsibilities of the Computer Science: Proceedings*, Volume 1, edited by P. Barroso Asenjo, T. W. Bynum, S. Rogerson, and L. Joyanes, (Madrid, Spain: Pontifical University of Salamanca in Madrid), 444–453.
6. WAGNER, I. LENOIR, N., QUINTANA TRIAS, O., MARTINHO DA SILVA, P., McLAREN, A., SORDA, M., HERMERÉN, G., HOTTOIS, G., MIETH, D., RODOTA, S., SCHROTEN, E. and WHITTAKER, P., 1999, *Ethical Issues of Healthcare in the Information Society*. Opinion of the European Group on Ethics in Science and New Technologies to the European Commission. Opinion 13, 30 July 1999. Online at <http://europa.eu.int/comm/sg/sgc/ethics/en/opinion13.pdf>, accessed 30 November 1999.
7. MAURO, V., 1999, Patient Privacy and Economic Interests: raising issues in health telematics. *ETHICOMP99 Look to the Future of the Information Society: Proceedings of the 4th ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communications Technologies*, edited by A. D'Atri, A. Marturano, S. Rogerson and T. W. Bynum (Rome, Italy: Libera Università Internazionale degli Studi Sociali Guido Carli).
8. SCHNEIDER, P., 1997 InSecurity: how safe are your data? In *Healthcare Informatics*, April 1997. Online at http://www.healthcare-informatics.com/issues/1997/04_97/safe.htm, accessed 09 March 1999.
9. ALPERT, S. A., 1998, Health care information: access, confidentiality, and good practice. In *Ethics Computing and Medicine*, edited by K. W. Goodman (Cambridge, UK: Cambridge University Press), 75–101.
10. UTILITY CONSUMER'S ACTION NETWORK, 1999, Fact Sheet # 8: How Private Is My Medical Information? Online at <http://www.privacyrights.org/FS/fs8-med.htm>, accessed 18 January 2000.
11. ANNAS, G. J., 1989, *The Rights of Patients: the basic ACLU guide to patient rights*, second edition. (Carbondale, IL, USA: Southern Illinois University Press).
12. NEVADO LLANDRES, M. A., 1998, Ethical problems caused by the use of informatics in medicine. In *Ethics and Information Technology*, edited by G. Collste, (Delhi, India: New Academic Publishers).
13. BARBER, B. and ROGERS, R., 2000, Response to comments on first working document on 'Guidance for handling personal Health data in International applications in the context of the EU Data Protection Directive'. Online at <http://forum.afnor.fr/afnor/WORK/AFNOR/GPN2/S951/PRIVATE/DOC/00033ann.pdf>, accessed 14 June 2001.
14. CAVANAUGH, T. A., 1999, Genetics and the fair use of electronic information. In *ETHICOMP99 Look to the Future of the Information Society: Proceedings of the 4th ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communications Technologies*, edited by A. D'Atri, A. Marturano, S. Rogerson and T. W. Bynum (Rome, Italy: Libera Università Internazionale degli Studi Sociali Guido Carli).
15. VLUG, A., 1999 Double encryption of anonymized electronic data interchange. In *ETHICOMP99 Look to the Future of the Information Society: Proceedings of the 4th ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communications Technologies*, edited by A. D'Atri, A. Marturano, S. Rogerson and T. W. Bynum (Rome, Italy: Libera Università Internazionale degli Studi Sociali Guido Carli).

16. BARROSO ASENJO, P., 1999, Ethical problems generated by the use of informatics in medicine. In *ETHICOMP99 Look to the Future of the Information Society: Proceedings of the 4th ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communications Technologies*, edited by A. D'Atri, A. Marturano, S. Rogerson and T. W. Bynum (Rome, Italy: Libera Università Internazionale degli Studi Sociali Guido Carli)
17. KLUGE, E.-H. W., 1998, Fostering a security culture: a model code of ethics for health information professionals. *International Journal of Medical Informatics*, **49**, 105–110.
18. GRITZALIS, D., TOMARAS, A., KATSIKAS, S. and KEKILOGLOU, J., 1990, Medical Data Protection: a proposal for a deontology code (HIDEC, Health Informaticians' Deontology Code). *Journal of Medical Systems*, **14**, 375–386.
19. CLAGETT, C., POVAR, G. and MORIN, K., 1996, Documenting sensitive information poses dilemma for physicians. In *ACP Observer* (December). Also at <http://www.acponline.org/journals/news/dec96/sensinfo.htm>, accessed 15 December 1999.
20. KLUGE E.-H. W., 1994, Health Information, the Fair Information Principles and Ethics. *Methods of Information in Medicine* **33**, 336–345.
21. DECEW, J. W., 1997., *In Pursuit of Privacy: Law, Ethics and the Rise of Tecnology* (Cornell University Press), as quoted p341 in Spinello and Tavani, 2001 [22].
22. SPINELLO, R. A. and TAVANI, H. T., 2001, Introduction to Chapter Four: privacy in cyberspace. In *Readings in CyberEthics*, edited by Spinello and Tavani (Sudbury, MA, USA: Jones and Bartlett), 339–348.
23. ORAM, A., 1999, A wronged individual. Message sent to email list med-privacy@essential.org. Online at <http://lists.essential.org/1999/med-privacy/msg00010.html>, accessed 09 March 1999.
24. KLUGE, E.-H. W., 2000, Professional codes for electronic HC record protection: ethical, legal, economic and structural issues. *International Journal of Medical Informatics*, **60**, 85–96.
25. PRIOR, M., ROGERSON, S., FAIRWEATHER, N. B., BUTLER, L. and DIXON, S., 1999, *Is IT Ethical? 1998 ETHICOMP Survey of Professional Practice* (Sidcup: Institute for the Management of Information Systems).
26. FLORIDI, L., 1998, Information Ethics: on the philosophical foundation of computer ethics. Paper at *ETHICOMP98*, but not present in *Proceedings of ETHICOMP98: The Fourth International Conference on Ethical Issues of Information Technology*, edited by J. van den Hoven, S. Rogerson, T. W. Bynum, and D. Gotterbarn (Rotterdam, Netherlands: Erasmus University Rotterdam). Online at <http://www.wolfson.ox.ac.uk/~floridi/ie.htm>, accessed 20 January 2000.
27. GOLDING, M. P., 1981, Obligations to future generations. In *Responsibilities to Future Generations: Environmental Ethics*, edited by E. Partridge, (Buffalo, NY, USA: Prometheus Books), reprinted from *The Monist* **56** (Jan 1972).
28. HOFELD, W. N., 1920, *Fundamental Legal Conceptions as Applied in Judicial Reasoning, and Other Legal Essays*, edited by W. W. Cook, (New Haven, USA: Yale University Press).
29. FIESER, J. and DOWDEN, B., (eds), 1998, Moral Personhood. In *The Internet Encyclopedia of Philosophy*. Online at <http://www.utm.edu/research/iep/p/personho.htm>, accessed 20 January 1999.
30. PAUL, L., 1999 Europe: managed care principles gaining ground. In *Healthcare Informatics*, March 1999. Online at http://www.healthcare-informatics.com/issues/1999/03_99/international.htm, accessed 09 March 1999.
31. *R v Mid Glamorgan Family Health Services Authority and another, ex p Martin* [1995] 1 All ER, 357.
32. GERARDI, L., 1998, Data Medical Privacy Act: an Italian lacking. Some remarks. In *Proceedings of ETHICOMP98: The Fourth International Conference on Ethical Issues of Information Technology*, edited by J. van den Hoven, S. Rogerson, T. W. Bynum, and D. Gotterbarn (Rotterdam, Netherlands: Erasmus University Rotterdam), 231–234.
33. KARANJA, S. K., 1995, *The Role of Legal Regulation in the Social Shaping of New Information Technologies: the computerised health data card (CHDC) as a case study*. Online at <http://www.uio.no/~stephenk/thesis.htm>, accessed 24 January 2000.
34. HAYS, M., 1997, A model for security. Sidebar in Schneider, 1997 [8].
35. SAFRAN, C. and GOLDBERG, H., 2000, Electronic Patient Records and the Impact of the Internet. Paper at *The 8th Working Conference of the IMIA WG4: Security of the Distributed Electronic Patient Record (EPR)*, Victoria, BC, Canada, 21–24 June 2000.