MEDINFO 2004
M. Fieschi et al. (Eds)
Amsterdam: IOS Press

Informed Consent to the Secondary Use of EHRs: Informatic rights and their limitations

Eike-Henner W. Kluge

University of Victoria and WG4 (Security and Confidentiality) IMIA

Abstract

It is frequently asserted that the secondary use of data contained in electronic health records (EHRs) requires the informed consent of the subjects of these records. This paper argues that while correct in principle, this has four important ethically based limitations: when it seriously threatens the equal and competing right of others, when it undermines the ability of health care providers to carry out their mandates, when it imperils the possibility of establishing and maintaining a health care system in the first place, and when it makes bona fide research impossible. Nevertheless, as a general rule, when consent can be had, it should be had. This paper provides a theoretical basis for these claims by looking at the nature and role of EHRs and provides some possible approaches for incorporating them into the health care delivery process.

Key Words:

Confidentiality, electronic health records, informed consent, secondary use of EHRs.

Introduction

One of the more troublesome questions that surround the establishment and use of electronic health records (EHRs) is whether it is ethically defensible to make non-consensual use of personal data for purposes other than those that were initially specified in their collection. The prevailing opinion seems to be that by and large, such secondary use requires the informed consent of the subjects of the records or of their duly empowered proxies.[1] This position can be argued in three ways: by citing the privacy rights of the subjects of the records, by claiming a contractual or quasi-contractual privacy arrangement between the subjects and whoever establishes the records, and by asserting a proprietary interest that subjects have in any personal data that originate with them.[2] The privacy rights tend to be grounded in the close association between the records and their subjects, and in the analogue role that EHRs play in information and decision space.[3,4] The claim of a contractual or quasi-contractual relationship prohibiting secondary use is supported by pointing to the confidentiality obligation that is inherent in the traditional health care professional - patient relationship and that has been expanded to the general health care setting;[5,6] Finally, the assertion of a proprietary interest is justified by appealing to the principle that whoever originates a product has a dispositionary right over it, and by arguing that the subjects themselves are the ultimate source of the information that is contained in their records.[3]

These three strands of reasoning enjoy varying degrees of validity. In particular, the third one requires extensive argumentation that pays due attention to the role of health care professionals in developing patient-centred information in the course of their professional interactions with their patients. Nevertheless, even if the arguments are granted, they are insufficient to establish that the non-consensual secondary use of patient data is always ethically objectionable and that informed subject consent is always required. In particular, there are four conditions under which such consent is not necessary: (1) when the use of the relevant data is integral to the health care professional or health care institution to carry out their respective mandates; (2) when failure to access and use the record would seriously jeopardize the equal and competing rights of third parties; (3) when access to the data contained in the records is necessary for *bona fide* and duly approved research purposes; (4) and when use of the data contained in the records is necessary for the development and maintenance of a health care system in the first instance.

However, before detailing the reasons for these exceptions, it may be useful to clarify the notion of what informed consent for the secondary use of patient data amounts to and how such consent should normally be achieved.

Informed Consent and EHRs

To begin with the notion of informed consent in the context of health care in general: Legally, although originally confined to the US setting, the notion has since become accepted in most jurisdictions and refers to the duty to disclose material information that patients should have before agreeing to or rejecting a particular course of action.[7,8] There are jurisdictional variations in the amount of information that should be disclosed and the level of sophistication at which such disclosure should be made - these are referred to as standards of disclosure and standards of comprehension respectively - but the core notion remains the same. Ethically, the concept is grounded in the principle of autonomy and in the individual's right of privacy, which in turn is grounded in the individual's right to the integrity of the person.[9]

Likewise, while the notion was originally developed in the context of the physician-patient relationship,[6,8] it has since been extended to all aspects of health care delivery including the domain of health information. Here it emerges as the patients' right to be informed that data about them are being gathered, stored,

processed, communicated, etc., and the right to give consent or refusal in this regard. It emerges further as the right to control the usage of data in all relevant contexts.[10]

The close relationship between the subject of health records and the data contained in them, as well as the traditional professional duty of patient confidentiality, make this extension of the notion of informed consent readily understandable.[11, 3] The expectation of consent to any secondary data use is further strengthened by the patients' belief that information about them that is developed in the health care encounter will be used solely for therapeutic purposes. This belief is generally not corrected or challenged by health care professionals or institutions, and therefore gives rise to a quasi-contractual obligation on part of the latter.

Limitations

However, even in its most liberal interpretation, there are some ethical limits to this right to informed consent for the secondary use of health information. The limits have a twofold root. These are, respectively, the principle of autonomy coupled with the principles of equality and non-malfeasance, and the principle of impossibility coupled with the principle of beneficence.

Autonomy, Equality and Non-Malfeasance

The principle of autonomy is to the effect that everyone has the right to self-determination; the principle of equality states that all persons are equal as persons and have the right to be treated accordingly; the principle of non-malfeasance asserts that everyone has a duty to prevent harm. [10,12,9]

In general ethics, the first two principles entail that the right to self-determination is subject to the condition that it may be exercised freely only if this does not interfere with the equal and competing rights of others. In informatic ethics it entails that the right to informatic autonomy is subject to the equal and competing informatic rights of other persons. Consequently, when withholding or blocking relevant data would imperil the equal and competing informatic rights of third parties, the legitimacy of such blocking or of such withholding has to be examined in light of these competing informatic third-party rights.[1] In other words, a balancing process is then called for.

The principle of non-malfeasance provides a means to effect such a balancing: If the subject's exercise of informatic autonomy (i.e., the insistence on privacy) would harm an identifiable third party or identifiable third parties to a greater degree than the harm that would be produced if the wish for privacy were to be ignored, then the privacy right of the subject of the EHR fails in this context and to this extent.

These considerations are reflected in the IMIA *Code of Ethics for Health Information Professionals* as the principle of legitimate infringement:[10]

> The fundamental right of control over the collection, storage, access, use, manipulation, communication and disposition of personal data is conditioned only by the legitimate, appropriate and relevant data-needs of a free, responsible and democratic society, and by the equal and competing rights of other persons.

Some Limits on Infringement

At the same time, while they do allow a breach of confidentiality, these principles also impose a limit on the nature and extent of any interference with the informatic autonomy rights of the subjects of EHRs. Specifically, such an infringement may never occur for the sake of mere convenience or efficiency, and it may not go beyond what is demonstrably necessary to safeguard commensurable competing rights or to prevent a greater harm.

This, also, is reflected in the IMIA *Code of Ethics*; specifically as the principle of the least intrusive alternative:

> Any infringement of the privacy rights of the individual person, and of the individual's right to control over person-relative data ... may only occur in the least intrusive fashion and with a minimum of interference with the rights of the affected person.

These limitations, therefore, capture condition (2) that was identified in the beginning.

Impossibility and Beneficence

The second basis for infringing informatic autonomy is grounded in the principles of impossibility and of beneficence. The principle of impossibility states that no-one can have a duty to do what is impossible, and the principle of beneficence says that everyone has a duty to advance the good of others.[9,10]

These principles affect the subject's informatic privacy and control rights as follows: Health care professionals and health care institutions require access to certain data that are necessary for them to allow them to carry our their respective mandates. Likewise, health care planners require access to certain data that are necessary for them to develop and maintain a health care system in the first instance. Therefore the principle of impossibility entails that if a patient enters the health care system in the expectation of treatment, the patient may not refuse *bona fide* access to the relevant data in her or his health record.

Likewise, the principle of beneficence entails that if access to certain data that are contained in a health record will advance the good of others (and if that good cannot be advanced in any other fashion) then there lies a *prima facie* duty to permit such access and, since this is an ethically grounded duty, informed consent is not required. The principle also entails that there lies a *prima facie* duty to permit duly authorized researchers to access patient data - since without such research, the quality of health care cannot be maintained or improved either for the patient her/himself or for any other patient. These conditions capture what were identified as conditions (1), (3) and (4) above.

Some More Limits

But again, the very principles that legitimate such an incursion into the patient's informatic rights[21] also severely constrain the extent and nature of such an intrusion. In every such instance, the incursion must be demonstrably necessary and not simply a matter of convenience. Further, while consent is not necessary in

---

1.2 Here as elsewhere, it will be understood that the subject's informatic rights may be exercised on behalf of the subject by a duly empowered proxy or substitute decision-maker.

these instances, autonomy and respect, coupled with equality and justice, entail that the subject of the record be informed of such an incursion if at all possible, and that prior notification of the possibility of such an incursion should be given at the time the health record is established so that the patient has the option not to engage the health care system under these conditions.

Moreover, here as elsewhere, when there is an abridgement of informatic rights, care must be taken *that* the data that are accessed in a non-consensual fashion be as de-identified as possible (principle of the least intrusive alternative), *that* whoever engages in such access be a *bona fide* authorized individual engaged in ethically legitimate activities; and, moreover, *that* this individual be legally bound not to communicate the relevant data to anyone who is not similarly legitimated. *As well*, there must appropriate security measures, inclusive of tight audit trails that are examined by an appropriately placed authority to ensure that the preceding conditions are strictly adhered to, and procedures must be implemented to test the effectiveness of these controls on a continual basis.[13] Without such limiting conditions, unconsented-to access to and use of the data contained in EHRs constitutes the informatic equivalent of voyeurism and trespass to the person. Finally, as an aside, it should be noted that these considerations may apply somewhat differently when the subject of an EHR belongs to a collectivity that defines membership in terms of communal and communitarian criteria. But even here, the central ethical considerations remain valid.

Some Policy Implications

To identify conditions of ethical acceptability is one thing, to express them as requirements of public policy and operationalise them in procedural terms is another. All too often, considerations of ethical nicety founder on the rocks of pragmatic reality. Therefore the question becomes, how to translate the preceding considerations into informatic protocols.

Here, one could proceed in several ways. One option might be called the *automatic authorised access model*. This would see an initial patient notification that data-access would normally be restricted to health care professionals who are actively engaged in providing care for the patient, but that patient data might be accessed for research, planning and related purposes by duly qualified and authorised individuals on a need-to-know basis without patient consent. There would be appropriate tracking and monitoring measures that would flag access by anyone other than a health care professional actively engaged in the care of the patient, to be reviewed by the data control officer of the relevant institution. The protocols would also require that the subjects of EHRs be notified of breaches in the informatic safeguards, so as to permit consultation about possible corrective and restorative measures.

This automatic authorised access model would have the advantage of simplicity. However, it would fail to acknowledge that if patients are willing to accept certain consequences (which will be outlined in a moment) they have an ethical right to impose access-limitations on certain identified types of data or to block access by certain types of individuals

A second model - what might be called the *modified automatic access model* - would involve processing all incoming data automatically into two streams: one that retains the data as entered, the other that strips them of identifiers as much as possible. Access to the identified data would be restricted to members of the care team - i.e., to individuals who stand in an immediate fiduciary relationship to the patient and are actually engaged in providing the patient with care; access to the de-identified data would be open without consent to duly authorized and accredited professionals in the domain of health care planning, research and delivery in general on a need-to-know basis. In each stream, all reasonable efforts would be made to safeguard confidentiality within the circle of the qualified and authorized professionals, all of whom would be under a legal obligation not to breach confidentiality. Here as elsewhere, automatic tracking, monitoring and breach-notification measures would be built into the respective protocols.

A third option - the *explicit consent model* - would be analogous to the consent protocols that are standard in health care interventions themselves.[6,8,9] Patients would be asked, each time that data about them are generated, whether these data may be accessed by duly authorised individuals who are not their immediate health care providers on a need-to-know basis, and under what conditions. Additionally, consistent with the principle of autonomy, patients would be given the option of limiting access to specific data in their EHRs to certain individuals that are (or that could reasonably be expected to be) engaged in providing care or, alternately, of blocking certain data to specified individuals or types of individuals. Clearly, this would have to be accompanied by an explicit and competent understanding that such limitation or blocking might jeopardize the possibility of receiving optimal (or even appropriate) health care, and that neither the health care professionals nor the health care system could be held responsible for any misadventure that might arise as a result of this.

A fourth, *two stage model*, might combine some of the features of the automatic and the explicit consent models in that it would expand the modified automatic consent model with the provision that access to identified data would be permissible to non-health care professionals upon explicit consent by the subject of the data.

Still other variations are possible. Indeed, current approaches such as the US HIPAA[14] model and the European Directive[15] mirror some aspects of the third and fourth model while differing in others. However, no matter how a specific model is developed, the central question is this: Does the model satisfy the fundamental principles of informatic ethics? Further, in light of contemporary research practices and patient mobility patterns, *any* model requires appropriate security provisions and accreditation and surveillance mechanisms; and in the global context, problems such as the interplay between the informatic rights of individuals who are embedded in ethnic or similar collectivities and the collectivities themselves will have to be addressed. However, one thing is clear: Not all secondary and non-consensual uses of EHR data are inherently unethical. Indeed, the principles of non-malfeasance and beneficence entail that all protocols, no matter what their specifics, should include override

functions that allow for non-consensual access even to identified data by duly authorized and qualified professionals on a need-to-know basis to protect the life and welfare of third parties; the principle of impossibility entails that informatic protocol should not make it impossible for health care providers and planners to fulfill their legitimate mandates; and the principle of equality and justice entails that informatic protocols should allow non-consensual access to safeguard the otherwise legitimate rights of third parties - such as the right to an appropriate defense in a court of law.

References

[1] Dierks C. Legal and social Implications of Health Telematics in the EU. In: Blobel B and Pharow P, eds. *Advanced Health Telematics and Telemedicine.* Amsterdam and Berlin: IOS Press, 2003.

[2] Gurry F. In *Breach of Confidence*. Oxford: Clarendon Press, 1995.

[3] Kluge E-HW. *The Ethics of Electronic Patient Records.* New York and Bern: Peter Lang, 2001.

[4] UK Information Commissioner. Guidance on the use and disclosure of Health Data. http://www.dataprotection.gov.uk/dpr/dpdoc.nsf 2002.

[5] Gillon R. *Philosophical Medical Ethics.* Chichester: John Wiley, 1986.

[6] Picard EI and Robertson GB. 3rd ed. *Legal Liability of Doctors and Hospitals in Canada.* Toronto: Carswell, 1996.

[7] Faden RR and Beauchamp TL. *A History and Theory of Informed Consent.* New York and Oxford: Oxford University Press, 1986.

[8] Stauch M and Wheat K with Tingle J. *Source Book on Medical Law.* London and Sidney: Cavendish Publishing Ltd., 1998.

[9] Beauchamp TL and Childress JF. *Principles of Biomedical Ethics*. 5th ed. Oxford and New York: Oxford University Press, 2001.

[10]IMIA The IMIA Code of Ethics for Health Information Professionals. http://www.imia.org

[11]Anderson JG and Goodman KW. *Ethics and information technology: a case-based approach to a health care system in transition*. New York and Berlin: Springer, 2002.

[12]British Computer Society (BCS). *A Handbook for Health Informatics Professionals.* Wiltshire, UK: 2003.

[13]Barber B, Allaert F-A and Kluge E-HW, Info-Vigilance or Safety in Health Information Systems. In Patel V, Rogers R and Haux R, eds. *Proceedings of the 10th World Congress on Medical Informatics* (London: IOS Press, 2001), pp. 1229-1233.

[14]Health Insurance Portability and Accountability Act (HIPAA) 1996, Public Law 104-191.

[15]EU Directive 95/46/EC; Data Protection (Amendment) Act, 2003; Directive 2002/58/EC , etc.

Address for correspondence

Eike-Henner W. Kluge
Dept. of Philosophy
University of Victoria
Victoria, BC, Canada
V9W 3P4
e-mail: ekluge@uvic.ca