

Counterpoint

Privacy and health information: the need for a fine-grained account

The privacy issue lies at the heart of an ongoing debate in nearly all Western democracies – the question is how to balance individual rights and collective goods. As far as the privacy issue in health care is concerned, liberalists tend to emphasize the importance of an individual moral right to medical privacy and informational self-determination, whereas communitarians typically argue that the community benefits from access to personal health data in terms of cost reduction, better medical research, improved public health and quality of health care. The liberalist view has become dominant in the Western world. Especially in Europe this has led to strong privacy laws which protect the individual. A recent report to the European Commission of the European Group on Ethics calls for further legal protective measures for health care data within the frame provided by the EU privacy directive of 1995 [1].

Don Detmer draws attention to the communitarian side of the controversy of the health data privacy debate. Like Amitai Etzioni he is concerned about some of the negative effects of the principle of informed consent as the centrepiece of European and most US privacy initiatives [2]. One of the negative effects is that the ability to review data for quality measurement in health care is seriously compromised by ‘opt out’ provisions at the discretion of individuals. Detmer’s argument amounts to a form of the public goods argument: medical science and quality health care are public goods, which require a steady (financial and informational) input and effort by all. If too many people ‘ride free’ by choosing anonymity and not making their health data available, then these public goods cannot be sustained and produced on an interesting level. This argument for limits to privacy and against opt-out controls aims at restoring a balance between individual privacy rights and the needs to know on the part of the community. It is in our common interest, Detmer suggests, to be less sensitive to the use of our medical data.

I agree with Detmer that the privacy issue will not simply go away and may become an obstacle in the relations between the USA and EU, as well as an impediment to quality measurement in health care. Detmer correctly points out that ‘much of the debate about the use of person-specific health information swirls around the *practical meaning of privacy* (my emphasis). I think that some of the hard privacy problems could indeed be resolved if this issue of the practical meaning of privacy would be addressed head-on and if we could be more precise about

the details of privacy questions. In order to be more precise we need to recast the ‘privacy versus health’ issue in terms of a more fine-grained account. The subject matter is too complex to be handled in terms of general notions such as ‘health data’, ‘privacy’, ‘confidentiality’, ‘doctor–patient relationship’. We need, for example, to specify which stakeholders and parties are involved [3], which specific normative rules of access are proposed [4], in which contexts medical information is created and in which contexts it is used [5,6], which different domains within (clinical, medical research, quality measurement, technology assessment, hospital administration) and outside (insurance, commerce, marketing, politics, criminal justice, accountancy) the medical sphere can be distinguished [7], which information exchanges across the boundaries of spheres and domains are allowed and which are not, which are the needs (to know, print, copy to, etc.) and (real and perceived) vulnerabilities of the relevant stakeholders, how their trust in the health care system is affected [8]. But first and foremost we must distinguish between the different moral reasons that may justify data-protection regimes for health data [9]. This will complete a fine-grained account of informational privacy in health care and will enable us to weigh competing claims more carefully.

The first type of moral reason for data protection is concerned with the prevention of harm, more specifically harm done to persons by making use of personal information about them. The fact that personal information is used to inflict harm or cause serious disadvantages to individuals does not necessarily make such uses violations of a moral right to *privacy*. In an information society there is a new vulnerability to information-based harm. The prevention of information-based harm provides the strongest possible justification for limiting access to medical records.

The second type of moral reason to justify data protection is concerned with equality and fairness. More and more people are aware of the benefits a market for personal data can provide. Many privacy concerns seem to have dissolved in *quid pro quo* practices and private contracts about the use and secondary use of personal data. But although a market mechanism for trading personal data seems to be kicking in, not all individual consumers and patients are trading their data in a transparent and fair market environment. Moreover they do not always know what the implications are of what they are consenting to when they sign a contract. Data protection laws in these

cases typically protect individuals by requiring purpose specification, openness, transparency, participation and notification to secure fair contracts.

A third type of moral reason concerns justice. The meaning and value of information is local, and allocative schemes and practices that distribute access to information should accommodate local meanings and should be associated with specific social spheres and settings. Many people do not object to the use of their personal medical data for *medical* purposes, whether these are directly related to their own personal health affairs, to those of their family, perhaps even to their community or the world population at large, as long as they can be certain that the only use that is made of it is to cure people from diseases or to improve the health care system. They do object, however, to their medical data being used to disadvantage them socio-economically, to discriminate against them in the workplace, refuse them commercial services, deny them social benefits, or turn them down for mortgages or political office. This amounts to a form of ‘informational injustice’, i.e. disrespect for the boundaries of what we may refer to, following Michael Walzer, as ‘spheres of justice’ or ‘spheres of access’. I think that what is often seen as a violation of privacy can oftentimes be better described as morally inappropriate transfer of data across the boundaries of what we intuitively think of as separate spheres of justice or spheres of access. Because of the peculiarities of the US health care system, which involves employers and insurance companies, this seems especially worrying [2].

I think that Detmer justifiably draws attention to the communitarian arguments in the health data privacy debate as a corrective to an unduly liberalist and individualist conception of persons and their privacy. The time has come now to start looking at the details and to identify the different

types of moral reasons for protecting health care data that both parties to the dispute can agree on¹.

Jeroen van den Hoven

Department of Philosophy
Erasmus University Rotterdam
The Netherlands

References

1. Wagner I. *Ethical Issues of Healthcare in the information society*. Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, No. 13, 30 July 1999.
2. Etzioni, A. *The Limits of Privacy*. New York: Basic Books, 1999.
3. Freeman P, Robbins A. The U.S. health data privacy debate. Will there be comprehension before closure? *Int J Technol Assess Health Care* 1999; **15**: 316–331.
4. Buckovich SA, Rippen HE, Rozen MJ. Driving toward guiding principles: a goal for privacy, confidentiality and security of health information. *J Am Med Informatics Assoc* 1999; **6**: 122–133.
5. Berg M, Goorman E. The Contextual Nature of Medical Information. Presented at the *Conference on the Impact of Information Systems in Health Organisations and Health Care*, Helsinki, 1998. Forthcoming in *Int J Med Inf*.
6. Nissenbaum H. Protecting Privacy in an Information Age: the problem of privacy in public. *Law and Philosophy*, 1998; **17**: 559–596.
7. Trappenburg MJ. Defining the Medical Sphere. *Cambridge Q Healthcare Ethics* 1997; **6**: 416–434.
8. Raab CD, Bennett CJ. The distribution of privacy risks: who needs protection? *Information Soc*, 1998; **14**: 263–274.
9. Van den Hoven MJ. Privacy and the varieties of informational wrongdoing. *Aust J Prof Appl Ethics* 1999; **1**: 30–43.

¹This research is at present carried out the departments of medical informatics and philosophy at Erasmus University Rotterdam by Lisette Eggink (supervised by Van Bommel, Van den Hoven and Van der Lei).