Personal Information in Medical Research

Response of the Foundation for Information Policy Research to the Medical Research Council's draft guidelines

1. The Foundation for Information Policy Research is an independent non-profit organisation that studies the interaction between information technology and society, with special reference to the Internet, from a broad public policy perspective; we do not represent the interests of any trade group. Our goal is to identify technical developments with significant social impact, commission research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

2. FIPR welcomes the MRC's consultation exercise, which addresses important issues in data protection, medical ethics and personal privacy at a time when these have become both difficult and important.

3. The risks of striking the wrong balance between patient privacy and research access to records can be seen in a number of other countries. For example, in Iceland, a government initiative to open up national medical records to genomic research has alienated the medical profession and led to a significant minority of the population opting out of the proposed genomic database. In such cases, it is quite unclear that the potential research benefits can outweigh the damage done to healthcare by the erosion of the trust relationships on which the practice of medicine depends.

4. In the UK, too, there has been considerable dispute between the medical profession and the Department of Health over the extent to which personal health information can be collected for secondary purposes without patient consent. The medical profession has strongly supported the GMC's line that 'patients have a right to expect that you will not divulge anything you learn in the course of your professional duties, unless they agree'; while the Department of Health has for some years maintained a doctrine of 'implied consent', namely that patients by the act of seeking treatment consent to any sharing of their information that officialdom finds to be convenient. This dispute is merely quiescent during the new government's honeymoon period, and could break out again at any time.

5. We are therefore surprised at the claim in section 2.2.6 of the draft guidance, that 'MRC has sought to base its guidance on a position that can command broad support, and is consistent with the view of the department of Health and the General Medical Council'. As noted above, the views of the DoH and the GMC are almost diametrically opposed on the issue of consent, and have been for over a decade.

6. We welcome the observation in Annex 4 that the laws on venereal diseases and human fertilisation make certain data flows completely illegal. The MRC should be aware that FIPR has a complaint outstanding with the Data Protection Registrar, to the effect that the arrangements whereby hospitals claim payment from health authorities for such treatments through the NHS Wide Clearing System (NWCS) contravene the relevant Acts. A data feed from NWCS to the Hospital Episode Statistics (HES) database also appears to contravene the Acts, and HES is used for research. There is a similar objection to the HIV data collection programme, under which the Public Health Laboratory Service collects identifiable data on HIV sufferers, both directly from the healthcare providers involved in their treatment and indirectly from laboratories which perform CD4 and other tests. FIPR has argued to the Registrar that these data flows constitute criminal offences under the relevant Acts. The Human Fertilisation and Embryology Authority has also taken the view that the central collection of identifiable data concerning human fertilisation in this way is illegal. The legal considerations for medical research cannot therefore be limited to the civil law of confidence, data protection law and the obligations imposed by medical ethics; the provisions of the criminal law must also be considered.

7. We are concerned however that the general drift of the MRC's document favours the utilitarian world view taken by the Department of Health, rather than the rights-based view found in the GMC's publications. For example, DoH guidance is quoted (in section 4.9.1 and elsewhere) but we see no citation of the comparable policy and guidance documents from the GMC or the BMA. Section 2.1.3 is a rather forceful statement of the DoH view; again, in section 2.1.4, consent is deemed to be desirable rather than mandatory; and section 2.1.5 contains a long list of possible reasons for not seeking consent. We find many of these arguments completely unconvincing. For example, if a GP does not have the resources to mail out a letter to several hundred

of her patients inviting them to participate in a study, the remedy is for the research team to pay her to employ additional secretarial help to work in her own practice under her own supervision, rather than to expect her to hand over her records to a research team to send out letters on her behalf. Given the nature of modern GP systems, this might mean giving the research team a copy of her practice database, or at least unrestricted access to it.

8. Although section 2.1.8 argues for the need to balance the competing claims of ethics and research, and section 3.1.5 states that MRC policy is to fund research to the level reasonably needed for the work to be done well, safely and ethically, the general impression that the guidance conveys is that there are many good excuses for not seeking consent – including poverty and inconvenience – and that so long as an ethics committee approves the proposed research, everything is fine.

9. While ethics committees may occasionally prevent abuses, they generally possess neither the technical nor legal skills to assess proposed security measures; their motivation to act as the patient's advocate is also in doubt given that they are typically staffed with the researcher's colleagues. One of the authors of this report has experience of rejecting, in his capacity as a learned journal referee, an epidemiological study in which blood samples taken to test for one condition were retested without consent for another – even in cases where consent for metabolic testing had been expressly refused. The test data had then been linked with census data to determine patient ethnicity, and were available to a number of research workers both inside and outside the research team before the results were finally de-identified and aggregated. When the ethics of this were queried, the authors of the study claimed that it had been approved by several ethics committees; they were very upset when the journal turned their paper down on ethical grounds and complained at the waste of public money. (Their work merely confirmed an already well known public health matter.)

10. In the great majority of cases, there is no reason why consent should not be sought directly. In the few cases where this is not possible, and researchers believe that they can make a strong case for the study to go ahead, we do not accept that the researchers themselves (or their colleagues on an ethics committee) should be the judges of this. Even with the best will in the world they are likely to be blind to everything but their project. We suggest that, as a minimum requirement,

a survey should be made of the attitudes of a statistically significant sample of the affected patients. Only if a large majority of them (perhaps over half those asked, or two thirds of those responding) approve of the research should it be permitted to go ahead. This could also be a useful clarification of the second bullet point of section 3.3.4. FIPR believes that no ethics committee should consider a request for non-consensual access unless presented with compelling empirical data that consent would have been given by a large majority of those affected. Without such a constraint, there will be a strong temptation for researchers to apply for non-consensual access simply because it is more convenient. The incentives should always push in the direction of ethical behaviour, or a moral hazard may be created which leads to systematic abuse.

11. In cases where consent has specifically been refused, that refusal must be respected unconditionally, unless explicitly overridden by statute. We find quite unacceptable the statement of section 2.4.5 that 'Explicit objections to disclosure should not, however, be a barrier to including anonymised information about the patient in pooled data or statistics.' It was recently held that anonymisation did not automatically discharge a duty of confidence [1] although this is currently under appeal. The point has been made by ACHCEW and others that it might be thought innocuous to de-identify the records of a woman being treated for an irregular menstrual cycle and include them in a study made for the purpose of developing safer oral contraceptives. However, her religious beliefs might absolutely preclude helping such research in any way at all. If despite her refusal of consent her records were used anyway, this would be a serious abuse of her trust. The same principle applies in more 'normal' cases. Here, too, we believe that the views of patients must be sought.

12. The MRC should pay particular attention to two surveys of patient attitudes to privacy conducted by the Fisher Medical Centre. The first [2] showed patients felt strongly that only practice clinical staff should have access to their GP records; they strongly disapproved of record sharing with other agencies both inside and outside government. The second [3] was directed at diabetic patients, a substantial majority of whom believed that they should be asked for consent before their detailed medical records are held on a regional register. A substantial majority also agreed that they should be identified on the

register only by a code rather than by their name and address. The patients' view may be summed up as 'anonymity plus consent', rather than 'anonymity or consent'. Such surveys suggest that patients are if anything more militant about privacy than doctors are, and it seems extremely unlikely that most patients would support the view taken in the draft, namely that de-identified data may be used against the express prohibition of a patient.

13. In cases where the use of de-identified data is approved, there still remains the issue of whether the de-identification is done competently, and following current Department of Health guidance is unlikely to be adequate. The Caldicott committee of enquiry into the use of personal health information in the NHS recommended that records be de-identified by replacing the patient's name and address with their NHS number, while also retaining their date of birth and postcode. Now as every NHS organisation needs to be able to map names to NHS numbers and conversely, this provides no protection; in addition, the combination of date of birth and postcode identifies some 98% of the UK population. (It seems scarcely believable that the Caldicott committee did not include either a computer security expert or a lawyer.)

14. We therefore feel that principles F and J in section 3.2 need to be expanded somewhat. What constitutes adequate de-identification? What security standards should be applied? Some useful guidance may come from the practices of the US Healthcare Finance Administration which uses two levels of anonymisation – 'beneficiary-encrypted' files merely have the names of the patients obscured, while in 'public-access' files enough of the patients' circumstantial data has also been removed for the re-identification of individuals to be highly unlikely [4]. Indeed, we would suggest that the MRC use this established terminology rather than introducing the equivalent terms 'encoded' and 'unverifiable' in section 4.5.1 – the US terminology is more explicit and less likely to lead to confusion.

15. Sections 4.5.6–4.5.10, which attempt to set standards for computer security, are too short for the purpose. Reference should be made to existing books (such as the BMA's policy document 'Security in clinical information systems' [5]) and standards (such as BS 7799); if the MRC wishes to write a booklet on computer security, it should be done properly.

16. One point that appears to be missing from the draft guidelines is that consent must be freely given. There are many factors in the NHS, from waiting lists to the disparity of knowledge between doctors and patients, which tend to make patients feel overawed and helpless in the clinical care setting. A patient connected to a heart monitor and a heparin drip in a coronary care unit is unlikely to feel able to say 'no' when the specialist registrar asks for a signature on a form stating that his records may be shared with a drug company doing a study with the cardiology department. Consent should be sought in such a way that patients do not fear for their relationship with their doctor (or their place on the waiting list) if they say no.

17. We can see no justification for the requirement in section 4.5.5 that a 'medically qualified person ... be in overall charge of identifiable medical information'. Even in the BMA's policy document, which in many respects takes the firmest line on medical privacy, the corresponding requirement is only that personal health information remain within the control of a healthcare professional. There is no objection to a pharmacist, or a nurse, discharging the duties of data custodian.

18. Some thought also needs to be given to the length of time for which records are to be kept. There are established rules on this, set out in the BMA document and elsewhere. If a record that would normally be kept only for eight years becomes part of a research exercise, then the guidance here would seem to imply that it must now be kept for 20 or even 30 years. The implications for data protection (and for the design of record keeping systems) need to be thought through.

19. We cannot agree with the guidance on sharing data with other groups which is set out in the two paragraphs numbered 4.8.4. Such data sharing should require consent to be sought afresh from the patients (unless it was explicitly contemplated when consent was first sought).

20. There are particular concerns when data start to be shared with large numbers of people rather than the relatively small number of people involved directly in the typical patient's care. As a general rule the probability that an information asset will be abused in proportional to its value and to the number of people with access. Aggregating data increases both of these risk factors at the same time. This is another reason why we are extremely uncomfortable with the idea of medical research teams accumulating copies of the identifiable records which

underlie many decades' research work. In extremis, the creation of too attractive an asset may lead to irresistible political pressure for access by interests whose primary motivation is not the welfare of the patient. The Iceland database, and the abuse of cancer registries by the security forces of the former German Democratic Republic, are merely two of the better known examples.

21. Finally, we question whether it is appropriate for the MRC to rush out new guidelines at the present time. Given that previous updates occurred at roughly ten-year intervals, and that the Latham judgment is about to be considered by the Court of Appeal [1], and that the regulations implementing the Data Protection Act 1998 are still awaited, it would seem more prudent to wait until the legal environment is less unstable.

References

[1] R v Department of Health, ex parte Source Informatics Ltd., QBD CO 4490/97, judgment of Latham J handed down 28th May 1999

[2] A Hassey, M Wells, 'Clinical Systems Security – Implementing the BMA Policy and Guidelines'. In Personal Medical Information – Security, Engineering and Ethics, R Anderson (ed), Springer 1997, ISBN 3-540-63244-1, pp 79–94

[3] M Wells, A Massey, A Wilson, D Pearson, 'Diabetic Registers: a practice survey of patients' attitudes'. In Health Informatics Journal v 4 nos 3-4 (Dec 1998) pp 216–222

[4] US General Accounting Office, 'HCFA Needs to Better Protect Beneficiaries' Confidential Health Information' (07/20/1999), T-HEHS-99-172, `http://www.gao.gov/AIndexFY99/abstracts/he99172t.htm`

[5] RJ Anderson, 'Security in Clinical Information Systems', published by the BMA (11th January 1996), `http://www.cl.cam.ac.uk/users/rja14/#Med`