

# Use of data from patient records for research: a model for best practice?

Nigel Mathers, Frank Dobbs

## Introduction

In the UK National Health Service (NHS), the registered list and the clinical records of patients are an invaluable resource for the quality assurance of clinical care in General Practice (e.g. audit) and for service development and quality initiatives. These records are also powerful instruments for the conduct of research in primary care. General practitioners are the “guardians” of these demographic and clinical data and, indeed, the use of patient data from these records for research in the past has given us many examples of excellent research which have had a direct impact on the care of our patients and the advice we give them.

For example, a classic study of over 40,000 people which linked GP prescriptions with data on hospital admissions and deaths was able to show a highly significant association between the use of minor tranquilisers (e.g. diazepam) and the risk of serious road traffic accidents. Patients were not contacted during this study and their clinical records were accessed without consent.<sup>1</sup>

The current policy of the Royal College of General Practitioners (RCGP) UK is that patients should be required to **opt in** to the use of their personal and clinical data for research projects rather than the alternative arrangements whereby patients are asked to **opt out** of participation in research projects. Such arrangements for the participation of patients in research have a direct impact, not only on the opportunities for research in general practice but also on the conduct of that research.

An example of the impact which ‘opting in’ and ‘opting out’ arrangements can have on participation in research may be seen in a recent study concerned with the management of patients with angina.<sup>2</sup> Half of the patients were randomised to ‘opting in’ whereby they only took part in the study if they got in touch with the researchers to say they wished to take part. The other half were randomised to ‘opting out’ whereby they were approached again by the research team and could decline to take part if they wished to. The ‘opt in’ route resulted in a lower participation rate and a **biased** sample with fewer coronary heart disease risk factors, less treatment and less disability as a result of their angina. The authors conclude that giving patients the opportunity to ‘opt out’ is a better method of recruiting a representative sample of patients than studies involving patients who ‘opt in’.

## The UK Academy of Medical Sciences report (AMS)

A recent Academy of Medical Sciences (UK) report “Personal data for public good: using health information in medical research” has stimulated the current debate on how **personal data** in routine clinical records may be used for research **without consent**.<sup>3</sup>

Personal data in this report are defined as data which relate to a living individual who can be identified from those data, and which can be used for medical research. Such data may include information on health (e.g. clinical data) or non-health issues (e.g. postcode or date of birth).

The AMS report highlights the present legal state of affairs in the UK where the law allows the use of identifiable data for medical research **without consent**, provided that such use is **necessary** and **proportionate** with respect to privacy and public interest benefits.

## Key words

patient, records, research

### Nigel Mathers\*

Professor of Primary Medical Care and  
Director of Academic Unit of Primary Medical Care,  
University of Sheffield  
Email: n.mathers@sheffield.ac.uk

### Frank Dobbs

Director of Postgraduate Medicine and Primary Care  
University of Ulster

\* *corresponding author*

In contrast to this approach, however, the professional colleges in the UK (e.g. the RCGP) have maintained a policy of requiring “**consent or anonymisation.**”

The question which needs to be considered now is whether this policy of consent or anonymisation should be reviewed in order to facilitate general practice research which could not be done otherwise, and if there is sufficient benefit to counterbalance any small reduction in privacy. This question is not about reducing the requirements for informed consent for invasive research which will alter the management of patients. It is about allowing the use of personal data held within routine clinical records for research, without the specific consent of the patient that it may be used for this purpose, but with safeguards to protect them from infringement of privacy.

### **Consent or anonymisation?**

The AMS report recommends that the safe use of identifiable data should rely on adequate **data security** policies rather than a policy of anonymisation. It also recommends that explicit consent to the use of identifiable patient data should always be sought in circumstances when seeking that consent is both feasible and proportionate. Where this is not the case, data should only be used within the context of a strict data security policy and in situations where the benefits outweigh possible disadvantages.

One of the issues which is raised by such a policy, however, is that of patients’ **trust** in their doctors – the annual MORI survey of UK residents in 2006, for example, revealed that the most trusted profession are doctors (92% of the population trust them) closely followed by teachers (88%). By contrast, politicians and journalists were only trusted by 20% and 19% of respondents respectively.<sup>4</sup> The doctor-patient relationship is one of the most important factors supporting high-quality care in general practice and trust is the central component of this. Clearly, the use of personal (identifiable) data from the clinical records of our patients for research purposes without consent could potentially threaten our relationship with our patients. Consideration of any policy changes, therefore, needs to place this concern at the centre of the discussion.

However, if such data security policies were to be introduced into general practice, it is clear that a model of **best practice** for data security needs to be developed – for example, not only by identifying how health records can be accessed but also by clearly stating who should have access to those health records and which data can be shared with non-clinical primary care researchers.

### **The case for research on anonymised record databases**

An alternative to using identifiable GP patient records for large population research is provided by the anonymised UK record databases General Practice Research Database [GPRD](10.1 million patients)<sup>5</sup> and QResearch<sup>6</sup> (about half the size of GPRD). Most epidemiological research which could

be done on identifiable records, can also be done on these anonymised databases. The GPRD data is downloaded regularly from 962 GP practices which use the “VAMP” Vision Patient Data Management System (PDMS). QResearch data comes from practices with the “EMIS” PDMS.

Tight control of permission to carry out studies is maintained by the organising bodies. Studies must be of acceptable quality and have a clear research question. Although database data are pseudo-anonymised, allowing updating of records over time, no identifiable data leaves the GP practice. Only subsets of data are released to researchers, sufficient to answer the specific question posed. Consequently the chances of infringement of confidentiality are minimised.

GPRD is available without charge to all health service researchers in the UK due to financial support from the Medical Research Council. QResearch is a not-for-profit organisation and charges a small fee for data access.

### **Engaging the public**

Consultation with patients and patient representatives reveals strong support for research using personal data at present, with confidence expressed in the integrity of research practices and their general practitioners. In a recent study by Barrett *et al* (2006), for example, on the use of medical records and registration for cancer research, interviews were carried out in a large random sample of UK homes. Participants were given a full explanation of the purpose of the research before being asked their opinion. The majority of participants supported the use of their personal data for cancer research and registration, provided confidentiality and security were assured.<sup>6</sup>

It is clear that if general practice research is to be carried out under a policy of data security as proposed by the AMS, then public engagement about the value of that research using health care records needs to be enlisted, and the arrangements under which records are held and accessed made explicit. This is particularly important with the advent of the NHS IT programme, ‘Connecting for Health’, whereby access to identifiable patient data (clinical records) will be available to health care workers in all parts of the UK as part of their clinical care.<sup>8</sup>

It is important, therefore, for primary care researchers and general practitioners not only to engage the public around the benefits of research involving personal data but also to demonstrate that high standards of confidentiality are consistently applied. Providing the public with specific examples of research which has directly improved the care of patients is also important. This can be supported by including such examples within a model for best practice in this area.

The robustness of the procedures for research governance and data handling must also be shared with people in the community, so that they can be happy with the balancing of confidentiality and the availability of data for analysis with improvements in health outcomes. There are, of course, many effective safeguards in place already to protect patients in

Europe from inappropriate use of their data in research. In the UK, these include the RCGP 'Research Ready' criteria and the current NHS Research Governance requirements.

## Good Practice Guidance

The AMS, the UK Clinical Research Collaboration (UK CRC) and the Medical Research Council (MRC, UK), along with a number of other concerned bodies are, at the time of writing, contributing to the development of a model for Good Practice Guidance which will 'encompass issues related to data security, anonymisation, consent and the use of health records to identify research participants'.<sup>3</sup>

Such guidance should provide not only practical guidance for practitioners but also a set of practical exemplars around which researchers can develop research proposals. This guidance could provide valuable assistance to general practitioners and other primary care researchers as well as to organisations involved with the governance and management of research in primary care.

For example, there are likely to be two major uses of identifiable patient data without consent in primary care research. The first is for **secondary research** on data collected for routine medical care, and the second is for the **recruitment of patients** to primary research studies.

Further examples can be found in the MRC guidance document on Personal Information in Medical Research.<sup>9</sup>

From this discussion, therefore, a model for good practice guidance for the use of patient data in general practice research is essential. The AMS report recommends that it should include the following components:

### 1. Data security and anonymisation

- Methods for data security (physical, technical and procedural security).
- Rigorous specification of who is appropriate to carry out anonymisation or pseudonymisation procedures and under what circumstances.
- Identification of who holds the encryption key and how access to data is managed.

### 2. Consent

- Methods for assessing the risk of introducing bias by requiring consent which may endanger the validity of results.
- Estimation of the proportion of a population who may be untraceable or not easily contactable to obtain consent.
- Assessment of overall financial and time burdens imposed and the risk of inflicting harm or distress by contacting people.

### 3. Use of health records to identify research participants

- Identification of the conditions and procedure by which health records may be accessed at start of research process.
- Specification of the mechanisms for contacting potential study recruits and for registering agreement or refusal to participate.

## The way forward

It is clear that a shift of policy from "opting in" or "opting out" of participation in research projects towards a policy which focuses on data security policies rather than consent or anonymisation issues has profound implications for researchers, practitioners and patients. The issues are complex even without detailed ethical consideration, but it is essential that we continue this debate right across Europe so that we can begin to develop some consensus on how identifiable ('personal') patient data can and should be used in general practice research without infringing the doctor-patient relationship.

## Acknowledgements

The authors are grateful to Professor Graham Watt, University of Glasgow, for stimulating debate on this issue and providing a framework within which informed discussion could take place.

## References

1. Skegg DC, Richards SM, Doll R. (1979). Minor tranquilisers and road accidents'. *British Medical Journal* 1979;7: 917-9.
2. Junghans C, Feder G, Hemingway J, Timmis A, Jones M. Recruiting patients to medical research: double blind randomised trial of "opt-in" versus "opt-out" strategies. *British Medical Journal* 2005;331:940.
3. Academy of Medical Sciences Report: Personal data for public good: using health information in medical research. <http://www.acmedsci.ac.uk/p99puid62.html>.
4. MORI Survey: <http://www.ipsos-mori.com/polls/>. Accessed 3 Jan 2007.
5. Why GPRD? <http://www.gprd.com/whygprd/>. Accessed 4 Jan 2007.
6. What is QResearch? <http://www.nottingham.ac.uk/~mczqres/whatis.html>. Accessed 4 Jan 2007.
7. Barrett G, Cassell JA, Peacock JL and Coleman MP. (2006) National survey of public views on use of identifiable medical data by the national Cancer Registry. *British Medical Journal* 2006;332:1068-72.
8. Connecting for Health: <http://www.connectingforhealth.nhs.uk>. Accessed 3 Jan 2007.
9. Guidance document on Personal Information Medical Research Guidance: <http://www.mrc.ac.uk/pdf-pimr.pdf>. Accessed 3 Jan 2007.