LESSONS FROM A 'PRIVACY IN HEALTH CARE' WORKSHOP, HELD IN THE COLLEGE ON 5 JUNE 2000

E. Russell, S. Cole, M. Bain, Privacy Advisory Committee, Edinburgh

The personal and health information collected about patients within the National Health Service (NHS) in Scotland is primarily used for direct patient care. However, much of this information can also be used to improve patient care indirectly through its uses for administrative, public health and audit research purposes. It is clear that, in general, members of the public have very little knowledge of the uses to which their medical information can be put other than for direct patient care. To attempt to address this issue the Privacy Advisory Committee (PAC) was set up by the Chief Medical Officer in 1990 to advise the Information and Statistics Division (ISD) of the NHS in Scotland and the General Register Office for Scotland (GROS) on privacy issues arising from medical research requests for individually identifiable data. A joint symposium of PAC and the Patient Liaison Group of the Royal College of Physicians of Edinburgh was held at the College on 5 June 2000. This symposium attempted to consider issues of privacy and confidentiality that PAC has found to be increasingly difficult in the light of recent legislation on data protection and human rights. In particular, it attempted to consider what the general public would regard to be acceptable and unacceptable uses of their health information.

A number of individuals representing consumer and patient organisations participated, as well as people who use data in research and audit.

NATIONAL DATASETS AND THEIR USES

There are many examples of the benefits of using personally identifiable health information. A good example is the Scottish Renal Registry. The care of patients with chronic renal failure lasts for the remainder of their lives and generates extremely bulky case-notes which give rise to storage problems and which often do not provide easily accessible information. The renal unit of the Western Infirmary, Glasgow, addressed this problem by buying a specifically designed software program in 1984, and by the following year, the notes of existing patients had been transferred, all the wards and outpatient clinics had been wired for terminals and doctors were entering observations during ward rounds and in clinics. Biochemistry results were directly downloaded from laboratories and a large part of the bulky paper case records had been abolished. The system was so successful that by the late 1980s most other renal units in Scotland had started to use the same system.

This computerisation of individual medical records was supported by the Scottish Renal Association, which consists of multidisciplinary representatives of the teams involved in treatment. Since then, the further development and extension of the information collected has involved consultation with the Association.

In 1990, when all the units had been computerised, it was realised that the pooled information could be used for planning and audit. A grant was provided by the Clinical Research Audit Group of the Scottish Health Department to purchase a central computer, based in Glasgow Royal Infirmary, to analyse data from each renal unit, and to employ an administrative assistant. The central computer is linked, through hospital networks, to each of the renal units' computers and can download information directly. The information analyses initially started with demographic and postcode data. It was also possible to audit individual units by returning to each its own data compared with the Scottish aggregate quality of care measures, such as the percentage reduction in blood urea during dialysis. This comparison was sent out twice a year for several years and between 1994–8 there was a marked improvement in the numbers of patients achieving the recommended target for blood urea reduction during dialysis. The audit of quality of care has been extended to other standards defined by the UK Renal Association and the Royal College of Physicians of London.

Not all standards can be assessed by objective measures, and now peer review by visiting groups of two nephrologists, a nurse and two patient representatives from another unit is being undertaken. This is a sensitive issue as it involves the patient representatives being given permission to have access to data about fellow patients and their documentation in the units being audited. A report is drawn up after a two day visit, and is sent to the unit, Trust and Health Board concerned. It is hoped that these reports and the other audit measures will play a part in clinical governance and the work of the Clinical Standards Board in Scotland (CSBS). Discussions are also being held with the General Medical Council (GMC) to see if the reports can help in the process of revalidation. In the context of concerns of the workshop, there are also other data linkages being undertaken: first, with the UK transplant waiting list and long-term follow-up of patients with a renal transplant, managed from Bristol and second, with the European renal register, which allows Scotland to be compared with other European countries in terms of outcomes. In the future, it would be advantageous to obtain information on the causes of death in renal patients for GROS and, more importantly, with the ISD who hold personally identifiable information on all hospital admissions. This would increase the knowledge of the patterns of disease and the care required by patients with chronic renal failure. Linkage with the cancer registry would also be an advantage, as patients with a transplant, on long-term immunosuppressive therapy are at greater than normal risk of developing cancer, particularly patients on long-term dialysis because chronic uraemia suppresses the immune response.

Another example, which demonstrates the research use of patient-identifiable information, is the MIDSPAN studies. The MIDSPAN studies started in the mid-1960s and involved

the long-term follow-up of people in middle age, from 45-65 years. They were started because of concern about the high incidence of cardiovascular deaths in young people in Scotland and the urgent need to learn about population risk factors. The populations chosen for study were from the Island of Tiree, factories in Clydeside and the towns of Paisley and Renfrew. The people were contacted, and the initial survey carried out at the time of mass miniature radiography screening for tuberculosis that was still done routinely in those days. In Paisley and Renfrew, Boy Scouts were persuaded to undertake a household census which gave important background detail, including aspects like passive smoking. People agreeing to take part were interviewed and medically examined for risk factors for heart disease and followed up periodically. Eventually the MIDSPAN study was extended to cancer by linking the study members to the cancer registry; later still also to mental health. When funding permits, the study subjects are contacted (and if necessary, traced using the NHS Central Register) and re-interviewed. On every occasion, from the earliest days, each person agreeing to take part gave written consent to examination and follow-up. The MIDSPAN study has now continued to the second generation, the middle-aged children of those original study members from the 1960s; extension to a third generation is being considered. This research to date has produced over 120 publications on health issues such as passive smoking and forced expiratory volume impairment as risk factors for cardiovascular disease, stroke, lung cancer, and Body Mass Index in relation to breast cancer.

DATA PROTECTION ISSUES

In considering appropriate uses of patient-identifiable information it is important to be aware of the main legislation and reports that are relevant to privacy issues. These are:

1. Data Protection Act 1998 (based on EU directive 95/46 (EC 1995));
2. Human Rights Act 1998;
3. Caldicott Report 1999;

In future, the forthcoming Freedom of Information Act will also be involved.

At the moment, the 1998 Data Protection Act is in a transitional period which will end on 24.10.2001, at which time it must be fully implemented, but the Act is still based on the original eight principles of the first 1984 Data Protection Act. It increases individual rights, covers paper records, and increases responsibilities of the data controller. The most relevant principle for the issue under consideration is the first:

> 'Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
>
> a. at least one of the conditions in Schedule 2 is met, and
> b. in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.'

The Schedule 2 and 3 conditions are shown in Figure 1.

FIGURE 1

The Schedule 2 conditions state –
All processing must meet at least one of the following conditions:

- have consent of the individual OR
- be required for carrying out a contract with the subject
- fulfil a legal obligation
- protect the vital interests of the subject (living or dead)
- carry out public functions
- pursue the interests of the service unless prejudiced to the interests of the subject.

The first condition means that the consent must be fully informed and freely given, and their consent can be withdrawn. Schedule 3 which applies to 'sensitive personal data' including health data requires further conditions before processing may be lawful.

Schedule 3 –

- explicit consent of the subject OR
- compliance with the legal duty
- protect the subjects' vital interests
- data already made public by the subject
- be necessary for justice
- for medical purposes
- other limited circumstances.

The medical purposes for which sensitive personal data may be processed include preventative medicine, diagnosis, research, medical management and provision of care and treatment. There is also a proviso that these data must be processed by a person with a duty of confidentiality (either professional or through their employment contract).

Article 8 of the Human Rights Act enshrines the right of everyone to respect for his/her private and family life, home and correspondence.

> There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedom of others.

The Caldicott Report on the review of patient-identifiable information in December 1997 applies to the non-clinical uses of NHS data. It recommended, *inter alia*, that patient identifiable information is transferred only for justifiable purposes and that only the minimum necessary is transferred in each case.

The interpretation of much of the new legislation is still being debated, and it is likely that some of it will be determined by test-cases in the courts. The safest course of action is to seek explicit informed consent whenever possible.

THE PATIENTS' PERSPECTIVE

The viewpoint of the patient is clearly important. There

are three main issues to be addressed:

- what do people know about the personal information held about them?
- what do they think about it; and
- does it really matter what they think?

There is a particular need for research into the first two questions, especially in view of the explosion in data linkage and central record keeping, as very little is actually known about general knowledge and belief about personal information.

The Data Protection Commissioner in her 15th Annual Report showed that 66% of people interviewed expressed concern about storage and use of personal information. The National Consumer Council found that people were uneasy and felt ignorant about the way personal information on them was being held and used.[1] They thought organisations should be open and tell them about it. In general, they were willing to trade personal information for a benefit to themselves. On the whole, people trust their doctors to keep their information confidential. What objections there are to computerisation relate to potential misuse, rather than to the development itself. There is also some concern about the potential for errors to occur in the actual recording of their data.

There are a few published papers of research[2, 3] which seem to show that people are not very concerned, and so, does it really matter what people think and believe – especially in view of the value that medical research has to the general community?

However, it may be dangerous to ignore patients' views. It is a matter of concern that the interests of the individuals' right to privacy is currently set in an adversarial way against the general good of medical research. Individuals, too, have an interest in seeing that good medical research is done and society has an interest in creating an environment in which individual rights are respected. If the adversarial mode of presentation is allowed to persist, the individual rights, now enshrined in law, may make epidemiological research more and more difficult. At the moment it appears that generally people trust their doctors to maintain confidentiality and this trust should be protected and safeguarded as far as possible. Figure 2 gives four ways of protecting the trust of patients.

FIGURE 2

Four ways of protecting the trust of patients:

1. consider carefully how to tell people what happens to their information. The best way to achieve this is not yet clear, but if we do not communicate with people, they will make up their own versions, based on anecdote or scare stories;
2. reassure people that the information will be kept as secure as possible;
3 publicise the safeguards which ensure that personal information is only used for proper purposes. These need to be established, and care taken to respect people's concerns;
4. take account of people's views when developing information systems. The involvement of patient representative in the Scottish Renal Register seems a very positive move.

It is important to appreciate that actual harm could arise from using personal information without explicit consent. It may prejudice full disclosure of relevant medical history by patients if there is a loss of trust in the medical profession to maintain confidentiality. There are also personal risks in being told certain things about oneself – e.g. genetic risk factors may have implications for obtaining life insurance or a mortgage. People should not be spied upon, which flagging and record linkage may verge on doing, but the general question as to what people think about privacy and the control of information is much in need of research. In such research, and in seeking informed consent, people must be told of the advantages to be derived from the good use of such data. But dangers lie in the very ease of data-handling and linkage leading to things being done that were unimagined a few years ago, e.g. what are people's views on being contacted to take part in research because of some illness they have had in the past, or because of an illness of a possible distant family member in the course of genetic research? People may not want to know about possible genetic risk factors.

WHAT ARE ACCEPTABLE USES OF PATIENT IDENTIFIABLE INFORMATION?

It is clear that there are very valuable uses of health information which indirectly contribute to improving health and health care. However, these uses need to be legitimate in line with what patients, and the general public, regard as appropriate and acceptable. Important unanswered questions include: what people currently understand happens to information about their health; what uses of such information, other than for direct patient care, can generally be considered acceptable; and are there clearly unacceptable research uses of patient-identifiable information?

The first principle is that we need to have a clear ethical framework within which to work. It needs to distinguish between different kinds of uses of information. Broadly these are:

- uses of anonymised information where an individual cannot be identified, and therefore there is no threat to their privacy;
- uses of information where an individual is actively participating in a research study and where the individual is specifically asked to consent to that use; and
- a range of uses of identifiable information which, in themselves, do not require contact with the individual (and do not therefore offer an obvious opportunity to gain consent), but which do involve using his/her information (a common example is casenote based research).

What different people find acceptable is not known, but the current legal position is that the first of these is legally permissible. The second requires explicit, informed consent, and therefore there is an integral opportunity for individuals to refuse. It is the last of these questions that most requires ethical debate and empirical research.

This framework also needs to consider the complex balance between the rights of the individual to control access to his/her information and the wider public health benefits of appropriate uses of health information. An important distinction exists between uses of personal health

information for the ultimate good of the general public versus uses of such information for private profit.

ACKNOWLEDGEMENTS

The Privacy Advisory Committee, ISD and GROS would like to thank all those who participated for their contributions. The Information Statistics Division and GROS are concerned to have the highest ethical standards in giving access to identifiable information and wish to assure themselves that their actions are publicly acceptable. The Privacy Advisory Committee will consider the implications of the discussions at this workshop in their continuing consideration of requests to use individually identifiable data.

REFERENCES

1 Tondel M, Axelson O. Concerns about privacy in research may be exaggerated. *BMJ* 1999; **319(7211):**706-7.

2 Denley I, Smith SW. Privacy in clinical information systems in secondary care. *BMJ* 1999l; **318(7194):**1328-31.

3 National Consumer Council. Consumer Privacy in the Information Age. London: NCC; 1999.