*21st April 2004*

# Patient Confidentiality in Scotland: an overview

**Dr Rod Muir**

## Background

1. The use and security of personal health data has received a great deal of attention in recent years as a result of several factors. These include increasing computerisation and networking of health information systems; changes to data protection law and professional guidance; and concerns about emerging public health issues such as HIV/AIDS and disease registers.

2. It is of vital importance to patients that their health data are kept secure and NHSScotland now puts considerable effort into systems designed to achieve this. It is also important, however, that those caring for patients should have access to the information they need in order to provide care.

### The drivers and the need to achieve a balance

3. NHSScotland (NHSS) and health services elsewhere have been engaged in debate over how best to achieve an optimum balance between individual privacy and sharing the information needed to provide 'seamless' care, measure quality, improve safety and plan and administer services (1).

4. The need for more data has been driven by consumer demand for better outcomes; by new inspection arrangements designed to increase accountability and by the desire of health planners to improve management efficiency and reduce waste. Consumers of health care have been encouraged to demand high standards and to know their rights, including their rights with respect to their information. The public are thought to know little about the ways in which their health data are used. (2). They may have anxieties about this information being passed on for surveillance, for marketing, insurance, commercial or research purposes, although little research has been done on this in the UK.

### Data Handling in NHSScotland

5. Large volumes of information are collected and held by the organisations making up NHSScotland. Hospitals, general practices, chemists, community care services and others gather and use information on patient contacts; diagnosis; procedures; drug treatments and so on in order to manage individual care; to track and monitor activity and assess the outcomes and quality of care and plan services. Most of the information used originates in individual person-based data. When used for planning or studying outcomes it is commonly 'anonymised' either by aggregation or by removal of obvious identifiers such as name and address in order to protect privacy but this not uniform and standards are just beginning to be agreed and applied.

6. Two organisations in NHSScotland are responsible for collating and holding large volumes of health-related data on individuals: the Information and Statistics Division (ISD), part of NHSScotland, and the General Register Office for Scotland (GROS). ISD gathers data from hospitals, general practices and other health care providers in order to provide national level comparative data and works with clinicians, policy makers and managers to provide the data they need for audit, quality improvement and operational management of health services. GROS is concerned primarily with the collation of data from the census and on deaths and other vital events. ISD and GROS exchange data e.g. on populations in order to calculate rates or to assess population shifts. Data are also provided to bona fide researchers by both organisations under closely scrutinised conditions.

7. The boundary between research, operational management and audit is often difficult to distinguish and both ISD and GROS rely on the advice of a Privacy Advisory Committee (PAC) in matters of this kind. This is of some importance as guidance from the Information Commissioner, from The Confidentiality and Security Advisory Group for Scotland (CSAGS) and from the General Medical Council (GMC) distinguishes between these uses of data and the kind of consent which each requires.

8. PAC is an informal advisory group with a predominantly non 'health' membership. Its status as such is under debate. Whilst it has been invaluable in providing guidance and independent scrutiny it is felt it needs to be more

accountable and visible and change status to meet the current standards for a public body. (see after)

**Increased complexity – new possibilities and new anxieties**

9. The complexity of information systems has increased rapidly in the past two decades. Networks of linked computers now collect, hold, analyse and transmit large amounts of personal information; electronic databases and registers are commonplace and play an important part in running health services; 'virtual' databases can exist within larger data sets, potentially subverting the rules on the use of registers; and datasets can be and are being linked electronically to create new knowledge. The benefits and risks of these activities are often hard to quantify. The relative values involved are often a question of perspective and the interests and rights of the individual may appear to be at odds with those of the larger social group. Whilst those in the field are aware of the need to inform the data subjects of the ways in which their data are used there has been little public discussion of the benefits and risks associated with this kind of data processing. This is familiar territory to those in the public health field and the current debate about the costs and benefits of vaccination are a good example of the difficulties involved in having a public debate about such an emotive topic.

**Current approaches to maintaining confidentiality**

10. NHSScotland has developed a number of systems for responding to legal and professional requirements on maintaining patient confidentiality. The main imperatives are the Data Protection Act 1998, the Common Law and current professional guidance, particularly that of the General Medical Council.

11. All NHS organisations have appointed a senior professional to be responsible for patient confidentiality, a 'Caldicott Guardian' (from the recommendations of the Caldicott Committee set up to advise on patient data handling in the NHS) whose role is to audit practice, manage an annual improvement plan and develop protocols for information sharing. This individual is a senior professional with access at board level who is there to ensure patient confidentiality is taken seriously at this level.

12. Organisations handling personal data must have a notification with the Information Commissioner which sets out what data they can process and for what purposes and these organisations are required to have a Data Protection Officer to assist in compliance.

13. Additionally, since organisations now depend heavily on IT systems to manage their data, many have appointed IT security officers.

14. Records managers also play an additional, important role in controlling access to patient records.

15. The chief executives of organisations failing to comply with the DPA98 risk being fined and imprisoned. Doctors and nurses failing to comply with professional advice on privacy issued by the General Medical Council (GMC) or the United Kingdom Central Council for Nursing, Midwifery and Health Visiting (UKCCNM) may have their right to practice removed.

16. Research uses of data are scrutinised in the United Kingdom by Research Ethics committees whose members are aware of data protection and privacy requirements, although this is not specifically part of their training and remit.

17. In Scotland the Privacy Advisory Committee (PAC) has been in existence for ten years to advise ISD and GROS on the use and release of personal health information. This was in recognition of the large volumes of personal information held by these bodies and the need for independent scrutiny of their stewardship of personal health data.

18. There is, however, currently no body in Scotland with the role of providing advice at national level on these issues and, when questions arise over interpretation of the law or professional guidance, the decision is ultimately one for the individual concerned. He or she must weigh the pros and cons of using or sharing the information in question and be prepared to justify this if challenged – a position which can be uncomfortable and one for which many doctors and nurses feel ill prepared. This may be inevitable given the current legal and professional regulations. The Scottish Executive Health Department is responsible for health policy and does provide advice and guidance on confidentiality from time to time.

**Recent developments**

**Confidentiality and Security Advisory Group for Scotland (CSAGS).**

19. CSAGS was set up in September 2000 as an independent committee, supported by the Scottish Executive Health Department (SEHD), to provide advice on the confidentiality and security of health related information to the Scottish Executive, the public and health care professionals. CSAGS reviewed the way the healthcare community in Scotland uses the information it collects from patients and reported in April 2002. CSAGS advised that changes in practice and culture were necessary if NHSScotland was to meet legal and ethical obligations to patients when using their health data. It concluded that patients knew little about the ways in which their data were used by the health services but also acknowledged that the future health of the population requires continuing access to this data.

20. CSAGS recommended that patients should be better informed as to how their data were used by NHSScotland and that much more extensive use of anonymisation and other privacy enhancing technologies should be made. The Scottish Executive was advised to promote training and an implementation strategy for all levels of NHSScotland. CSAGS recommended against new legislation permitting the processing of health data. This was to remain as a contingency.

21. The implementation of CSAGS recommendations has created a considerable work programme in Scotland that is likely to increase the demand on Caldicott Guardians and others involved in information security.

**Scottish Executive Health Department Response to CSAGS**

1. The Scottish Executive Health Department (SEHD) outlined its response to the CSAGS recommendations in August 2003 setting out a work programme to "promote best practice and continued improvement in the use of personal health information as an integral part of patient care." (3) It retains the responsibility for standards of patient confidentiality within the framework of clinical and staff governance and clinical risk; "recognises and supports"

Caldicott Guardians as leaders for this "challenging agenda" and sets out milestones to progress and priority tasks against which progress is to be reviewed in April 2004. It emphasises the need to inform staff, patients and the public, and to seek appropriate consent for the use of data.

2. At the same time a new Code of Practice for NHSScotland on Protecting Patient Confidentiality has now been introduced (4); local patient information leaflets on protection of personal health information are being issued by NHS Boards and Trusts and NHS organisations are asked to use anonymised national data where appropriate and to set up systems to similar standards for local data flows. The SEHD also called for a review of staffing and support for Data Protection and Records Management.

**Some current areas of difficulty**

**Disease registers**

3. A register is, at its simplest, a set of organised information that is kept up over time. The means of storing the information will range from paper (e.g. index cards or a book) to computerised databases; their size will vary from a few to millions of records and they may be kept by, or for, individuals, groups of individuals or organisations. Their status will vary from small and informal to large and officially recognized. Some have a legal basis e.g. Census data but most do not.

4. The original written type of register is now being replaced by computerised systems and this has fundamentally changed their nature. For example the data included can be analysed more quickly and in more sophisticated ways. Also now a 'register' of individuals sharing common features can exist in 'virtual' form as an easily accessible subset of a larger collection of data collected for a wider purpose. The actual location of the data is now relatively unimportant; what matters is who controls the data and who has access to it. A population database can be held on a computer in Dundee but be accessed and managed by staff in Edinburgh. Data in one register may be linked to data in other registers. An example of this is the linkage of National Health

Services Central Register to Vital Events data, to the Community Health Index and to the Cancer Registry.

5. Registers have a number of uses in health and social care (5): preventive medicine; genetic counselling; follow up and treatment; population registers; at risk registers. Some are disease specific, some person specific and some function specific.

6. In order to be useful the data collected needs to be accurate and valid. For some purposes *completeness* of data is important (e.g. for immunisation programmes or determining disease incidence and prevalence) Registers need therefore to be administered and maintained. The problems this presents vary with the size and complexity of the data, and its intended use. Clear definitions and inclusion criteria are required, quality assurance systems are needed if data quality is to be maintained and the reasons for collecting the data need to be clear and the uses of the data need to be justified. This clearly presents challenges for those maintaining registers.

7. There are a number of ways in which good practice could be developed and ensured e.g. through education: standards; enforcement and inspection; audit, quality assurance and professional accreditation. All are likely to be either costly or bureaucratic, or both. This clearly should be part of a wider approach to governance of information use.

**Consent, informing and opt out**

8. Inadequate and confused guidance over these issues causes uncertainty for those processing personal data.

9. In the case of consent, data processors are often informed that consent 'must always be obtained' but guidance commonly fails to make it sufficiently clear that consent may be implied in many circumstances e.g. when data are being processed for operational management of a service carrying out legitimate functions. This is a potential criticism of the current guidance from the General Medical Council, which is set out in terms that many doctors find threatening. (This has recently been revised and issued with a set of "frequently asked questions")

10. As regards information giving, it is now more widely appreciated that data subjects must be advised that their data are being processed if processing is to be fair and legal. Health services are now working to conform to this. However there is little clarity as to what level of information is required, or how it should be provided. The Information Commissioner is likely to require only that organisations are making a reasonable attempt to improve information giving over a realistic time period but the lack of guidance on standards leaves room for uncertainty.

11. Lastly, guidance commonly gives the impression that those patients who do not wish to have their data processed have an automatic right to prevent this. However, the Data Protection Act 1998 states (Section 10) that an individual is entitled to require a data controller not to process any personal data in respect of which he is the data subject only for specified reasons:- (a) the processing of those data or their processing for that purpose or in that manner is causing or is likely to cause substantial damage or substantial distress to him or to another, and (b) that damage or distress is or would be unwarranted.

12. As Lowrance (6) has pointed, the right to privacy is not absolute. "The Data Protection Act ensures that data-subjects have a right to inspect data about themselves, which contributes to patient-centering of care. But although it may give the patient a photocopy or printout, or correct an error or insert an amendment at a patient's request, for a variety of medical and legal reasons no health provider… can relinquish possession of, or right of control over, data it has collected in providing or paying for care."

13. If this were more widely appreciated it would avoid some of the confusion and uncertainty surrounding data processing.

**Anonymisation**

14. CSAGS proposed that all data used for secondary purposes should be 'anonymised'. The attraction of this approach is that, in theory, once data are anonymised they are no longer regarded as personal data (i.e. identified with a living individual) However, although CSAGS proposed that the removal of

name, address, full post-code and full date of birth would constitute 'acceptable anonymisation' for most purposes, there is as yet no generally accepted definition of 'anonymisation' or 'acceptable anonymisation'.

15. In practice neither individual data items nor data sets can be neatly categorised as either person (or patient) identifying or anonymous. Single data items reveal little, although some identifiers are regarded as more obviously identifying than others, particularly name, address, full date of birth and full postcode.

16. Multiple data items or datasets, on the other hand, present greater or lesser risk of identifying individuals depending on the data items they contain and the context. Some data sets clearly carry a high risk of identifying individuals, especially if they contain any of the more obviously identifying fields listed above, whilst some present little risk. A continuum of risk exists between these extremes and it is often difficult to know where a given set of data lies on this risk spectrum. Consequently, those involved in handling patient data need to exercise skill and judgment and they require robust systems and useable pragmatic guidelines.

17. 'Anonymisation' is a complex set of processes made up of people and systems and involving data transmission, data holding and data access controls. Even after obvious identifying data items such as name, address, full postcode and date of birth are removed from data sets the risk of 'indirect' identification of individuals remains and even such partly 'anonymised' data have to be handled securely. The challenge is to balance the risk of using the data against the benefits to the patient or the care 'system' of using them e.g. in efforts to improve the quality of care. The processes and systems on which all this relies need constant scrutiny and improvement if they are to work effectively.

**Conclusion**

18. The debate over the use and safeguarding of personal health information goes on; the issues are complex, but there are signs of a consensus emerging in some areas (1). However in others doubts remain: e.g. over the clarity of professional guidance and how to achieve consensus over its interpretation;

how to inform patients and what to tell them; how to regulate disease and other registers; whether it is possible to 'anonymise' data in ways which retain their usefulness.

19. The current arrangements in Scotland have grown up in response to what often seems to those involved to be a forest of regulations with only occasional clearings of common sense. Some pathways through this are emerging. Those responsible for exploring them are keen to have the issues debated more widely and to have help with seeing more of the wood and less of the trees.

**References**

(1) Chalmers, J, Muir R. Patient privacy and confidentiality. *BMJ* 2003;**326**:725 -6

(2) Confidentiality and Security Advisory Group for Scotland. *Protecting Patient Confidentiality-final report.* Edinburgh: Scottish Executive Health Department 2002

(3) *The Use of Personal Health Information In NHSScotland To Support Patient Care.* Edinburgh: Scottish Executive Health Department, 2003

(4) *NHS Code of Practice on Protecting Patient Confidentiality*. Edinburgh: Scottish Executive Health Department 2003 (www.show.scot.nhs.uk/confidentiality )

(5) Weddel JM. Registers and Registries: A Review. Int J Epidemiol 1973; **2** (3): 2218

(6) Lowrance WW. Learning from experience: privacy and the secondary use of data in health research. London; Nuffield Trust 2002