

The Confidentiality & Security  
Advisory Group for Scotland

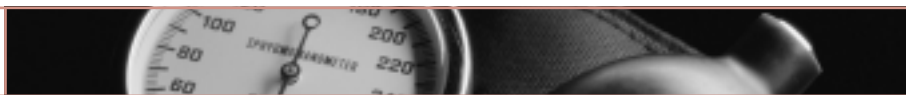


**PROTECTING PATIENT CONFIDENTIALITY**  
Final Report



## Final Report

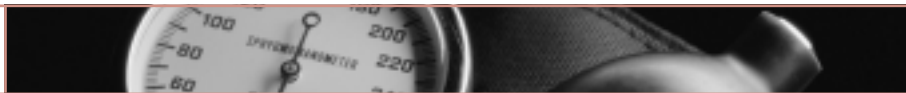




## CONTENTS

1	FOREWORD	4
2	INTRODUCTION	6
3	PROTECTING THE RIGHTS OF THE INDIVIDUAL – THE REGULATORY ENVIRONMENT	8
4	USES OF PATIENT IDENTIFYING INFORMATION – OBLIGATIONS OF NHSSCOTLAND AND INDIVIDUALS	12
5	THE WAY FORWARD	17
6	INFORMING THE PUBLIC AND PATIENTS	19
7	OBTAINING CONSENT	24
8	ACCEPTABLE ANONYMISATION	32
9	SECURITY OF HEALTH SERVICE INFORMATION SYSTEMS	37
10	NEW LEGISLATION	38
11	DELIVERING CHANGE	42
12	THE PRINCIPLES OF CONFIDENTIALITY	44
13	SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS	46
A	ANNEX CSAGS – AIM, TASKS AND COMPOSITION	51
B	ANNEX DEFINITIONS AND GLOSSARY	52
C	ANNEX CONCLUSIONS AND RECOMMENDATIONS FROM THE ACCEPTABLE ANONYMISATION FEASIBILITY STUDY	54

- 1.1 This Report to Scottish Ministers has been prepared by the Confidentiality and Security Advisory Group for Scotland (CSAGS). 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'. Full details of our terms of reference, membership and web site are given at Annex A .
- 1.2 In the light of changing legal and professional requirements and of the need to ensure full partnership with patients in healthcare services, we have undertaken a wide-ranging review of the way the healthcare community in Scotland uses the information it collects from patients. In the summer of 2001 we published our consultation paper 'Protecting Patient Confidentiality: A Consultation Paper', which contained a draft strategy and proposals for change. That paper was widely circulated and supplemented by a series of roadshows covering each NHS board area.
- 1.3 We received some 150 responses to the consultation, almost all from organisations and individuals from within the Health Service. Copies of these responses are available from the Scottish Executive Library at Saughton House. (Those unable to attend the Library in person can request copies on 0131 244 4551.) Because the response from the public was limited, we arranged two pilot sessions for focus groups in the Argyll and Clyde Health Board Area to provide feedback on the major issues. Whilst acknowledging the limitations of this project, it nevertheless gave us an indication that the public want to know how their personal health information is used and to share in decisions about its use. If this happened, most people at the focus groups supported its use for the benefit of the health of the population.
- 1.4 There is no doubt that changes in practice and culture are required so that NHSScotland can fully meet legal and ethical obligations to patients when using their health data. There is also no doubt that the future health of the population requires continuing access to these data by healthcare professionals. The major task for CSAGS has been crafting proposals which take full account of these imperatives and provide workable solutions which will both meet the needs of patients for more involvement and better information when their data needs to be used, and the concerns of health professionals who need reassurance that essential flows of data will still be available to them.
- 1.5 The recommendations in this Report address these and many other issues. Changes are needed to move procedures forward to meet best practice standards, which must be the aim. We know this will take time. In the meantime there are clear minimum standards which should be achievable now, including the provision of better information to patients and the universal adoption of a working practice within the NHSScotland of always questioning the need for any data collected or shared to be patient identifiable.



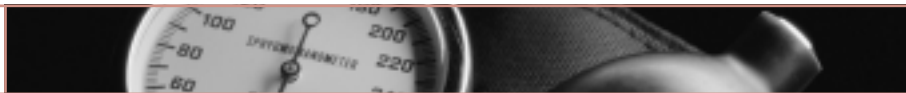
## Final Report

1.6 With the presentation of this Report to Scottish Ministers, CSAGS has now completed the task it was set. We very much hope that our proposals will be endorsed and implemented. We refer, in the Report, to the need to review progress on the implementation of our proposals, to monitor their effect and to advise and adjudicate on any unresolved issues. Consideration will need to be given to the creation of an independent body to undertake such tasks and to provide future advice to Scottish Ministers.

1.7 The expertise and experience of CSAGS members and the invaluable assistance of our Secretariat contributed much to our review and to this Report. We have also valued the views of staff from the Office of the Information Commissioner and other key organisations, such as the General Medical Council. Many of the responses to our consultation were challenging and helpful. Our thanks go to all who have contributed.

ANGELA MACPHERSON  
CHAIRMAN, CSAGS  
25 APRIL 2002

- 2.1 NHSScotland depends for its existence and efficient running on information collected from those who use its services. That information sometimes has to be shared between several people or services. At its most basic, information about a patient's condition is shared between those staff caring for an individual so they can meet a patient's specific needs. Information from patients is also used to plan and run services. For example, information is required to operate appointment systems and inpatient waiting lists. Learning how to improve care also relies on information about patients and their treatment.
- 2.2 Most people will be aware of the sheer complexity of an organisation like NHSScotland and its need for information in order to function. What is less likely to be well known however, is the amount of detail about individual patients that is needed. For example, it is necessary to know the name, age and address of women, who are eligible for breast or cervical screening, so that they can be invited for screening at the right time. Also less well known is the extent to which key public health functions depend on the ability to put together information about a single person which has been drawn from a variety of sources such as laboratories and clinics.
- 2.3 The use of information about individual patients is governed by:
- statute law eg the Data Protection Act 1998 and Human Rights Act 1998;
  - the common law on privacy and confidentiality;
  - professional standards; and
  - organisational codes of conduct.
- 2.4 These are described in more detail in section 3. They combine to require users of data to be transparent, accountable and responsive to the needs of individuals.
- 2.5 Best practice has been evolving. In healthcare, improvements in practice have come from the Caldicott Committee's Review on Patient-Identifiable Information (1997), and changes to standards set by professional bodies. The main task of CSAGS is to advise how the procedures of NHSScotland match up to current legal, professional and ethical requirements on confidentiality and security and to make proposals on best practice.
- 2.6 CSAGS' goal is for a Health Service that protects privacy and thus:
- commands the support and confidence of users and staff;
  - complies with best practice;
  - conforms with the law; and
  - does not unduly restrict patient care, the running of the organisation, or the improvement of health and care through new knowledge.



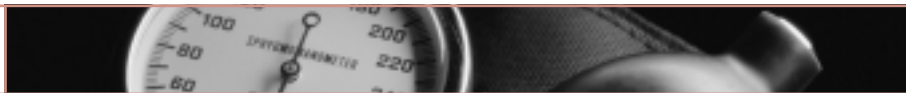
## AN ETHICAL PERSPECTIVE ON PRIVACY

- 2.7 Individuals should be able to expect that information about their health which has been given in confidence, will be kept private unless there is a compelling reason why it should not. The principle of a confidential relationship between a patient and a clinician is an ancient one, shared by many cultures.
- 2.8 This principle holds insofar as an individual is autonomous. In some situations, one person's claim to privacy could infringe the competing claims of others who for example as patients, wish to benefit from useful research or to avoid communicable diseases and who as tax-payers, wish to support an efficient and effective health service.
- 2.9 Where a person's claim to privacy has little or no effect on others, then there is a clear ethical duty of confidence. This is implemented in law, particularly common law (which is based on previous judgements in the Courts), and in the guidance on ethical conduct published by professional bodies.
- 2.10 What is less clear is how a public duty interest impinges on the privacy interests of the individual; ie to what extent can individual rights to privacy give way to the health benefits of society as a whole. This tension may sometimes be decided by law and sometimes by debate. What is important is that individuals are aware of the issues, so that they are able to play an informed part in that debate.

- 3.1 Patient identifying information is defined as a data set which may include some or all of the following: a picture of the patient, the patient's name, address, full post code or date of birth. As we explain in section 2 the use of patient identifying information by NHSScotland is subject to:
- statute, in particular the Data Protection Act 1998, the Human Rights Act 1998; the Infectious Disease (Notification) Act 1889 and the Abortion Act 1967;
  - the common law;
  - standards set by professional bodies; and
  - the policies and organisational standards of the Scottish Executive Health Department (SEHD) and NHSScotland.

### DATA PROTECTION ACT 1998

- 3.2 The Data Protection Act 1998 came into force in March 2000. Its purpose is to protect the right of the individual to privacy with respect to the processing of personal data. As far as NHSScotland is concerned, a key requirement is in Schedule 1 of the Act. This requires organisations to process fairly and lawfully any information which might enable a patient to be identified.
- 3.3 To be **fair**, organisations must comply with the Fair Processing Code. Amongst other things, this Code requires patients to be informed of the identity of the 'data controller'. The term 'Data Controller' is used in the 1998 Act to describe organisations that process personal data. In the case of NHSScotland, data controllers will be the organisation that collects information from patients. It might be a general practice, a NHS Trust, a NHS Board or a Special Health Board. Responsibility for complying with the 1998 Act rests with each organisation as a whole, with chief executives bearing the ultimate responsibility for the actions of their staff. Other requirements of the Fair Processing Code are dealt with in detail in section 6 of this report.
- 3.4 In order to be **lawful**, the Information Commissioner takes the view that data controllers must comply both with statute and with the common law. This has a bearing on the need for patients to give consent before patient identifying information is shared.
- 3.5 The requirement to process data fairly and lawfully is not the only requirement of the 1998 Act. For example, the Act requires organisations that wish to process patient identifying information to use the minimum amount of information necessary and to retain it only for as long as is needed for the purpose for which it was originally collected. This is referred to as the Third Data Processing Principle. Draft guidance on the retention periods for health records has now been published for consultation by SEHD and can be found on [www.show.scot.nhs.uk](http://www.show.scot.nhs.uk).



- 3.6 A guide to the Data Protection Act 1998 is available from the Office of the Information Commissioner at: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel: 01625 545700 or on the Web at [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk).

### THE HUMAN RIGHTS ACT 1998

- 3.7 This Act implements the provisions of the European Convention of Human Rights (ECHR). Article 8 of the ECHR guarantees respect for a person's private and family life. Disclosure of personal medical information would be a breach of that right unless it was 'in accordance with the law' and necessary for the protection of health. This means that patient identifying information should not be disclosed unless there is a lawful basis to do so, such as the consent of the patient, compliance with a legal requirement or the need to protect life.
- 3.8 An example of the need to comply with a legal requirement is the Infectious Disease (Notification) Act 1889. This Act requires that in the interests of wider public health, both relatives and practitioners who become aware that someone is suffering from a notifiable disease (such as measles or chickenpox) must notify the local Director of Public Health of that fact.

### THE COMMON LAW

- 3.9 The common law in Scotland is based on precedent. As a result its impact is not always clear and it may change over time. Whilst various interpretations of the common law may be possible, there is widespread acceptance that it reinforces the need to obtain consent from patients before sharing information about them.

### PROFESSIONAL STANDARDS

- 3.10 All healthcare professionals must maintain standards of confidentiality laid down by their professional body, such as the General Medical Council. As a rule, such standards have been developed to clarify what the law means in a healthcare setting and to set out any additional principles or ethical standards for that profession. NHSScotland must ensure that its systems and procedures enable healthcare professionals to comply with the requirements of their professional body.

### POLICIES AND ORGANISATIONAL STANDARDS

- 3.11 CSAGS understands that the Scottish Executive aims to ensure that patients are fully involved in decisions about the use of information about them and that information provided by patients is kept confidential. A wide range of organisational rules and standards already exist to support this policy. An important example is the Caldicott Framework that was set up in March 1999 to respond to the recommendations of the Caldicott Committee in its 'Report on the Review of Patient-Identifiable Information'. The Framework requires each

NHSScotland organisation to appoint a senior clinician such as the medical director as 'Caldicott Guardian'. The Guardian's responsibility is to:

- audit current practice and procedures;
- manage an improvement plan which will be monitored through the clinical and corporate governance frameworks; and
- develop protocols for inter-agency information sharing at a local level.

3.12 In addition to these functions, Caldicott Guardians are involved in making decisions about how their organisation uses patient identifying information. For instance, it will be the Caldicott Guardian who decides whether to provide patient identifying information to a health research project. The Caldicott process is now under review and CSAGS expects that over the summer the Health Department will work with NHSScotland on a new system for ensuring that local organisations meet the broader confidentiality standards expected of them. This will include a new framework for making decisions on using data where more than one NHS organisation is involved.

3.13 All NHSScotland employees and contractors are contractually obliged to respect a patient's right to confidentiality. It is policy that all members of staff are provided with a copy of the Code of Practice on Protecting Patient Confidentiality. Failure to comply with the Code of Practice is a disciplinary offence.

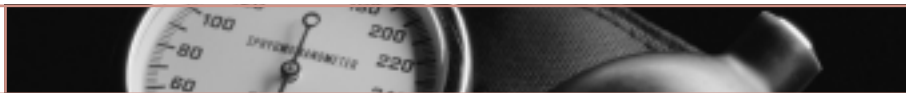
3.14 There is also a series of rules for specific situations such as the use of faxes for confidential information, the retention and storage of records and IT security. CSAGS understands that NHSScotland is reviewing these documents to confirm that they take into account data protection and human rights legislation.

### INTER-AGENCY CARE

3.15 Patient care often involves health and social care organisations. NHSScotland undertakes joint work with a variety of agencies, on a mix of health and social care problems which face many patients. The managed sharing of patient identifying information necessarily accompanies these day-to-day activities, and any effective strategy for preserving patient confidentiality must embrace this.

### RESEARCH

3.16 Local research ethics committees in each NHS area and a multi-centre national committee are responsible for ensuring that all research meets agreed ethical standards. Research ethics committees provide an additional check that research projects respect patient confidentiality and meet requirements on consent for uses of identifiable information.



3.17 At a national level, the use of data by The General Register Office for Scotland (GROS) and Information and Statistics Division (ISD) of the Common Services Agency (CSA) is scrutinised by the Privacy Advisory Committee. This is an independent body, set up to advise on the release of any health data which are potentially identifying. The Committee consists of a professor of public health, a clinician, and three lay members. New requests for ISD or GROS to release data are examined by the Committee, using the '3R' principles. These are:

- **replacing** patient identifying information with other material when this is appropriate;
- **reducing** the use of patient identifying information to a minimum when it does have to be used; and
- **restricting** access to only those who require it.

3.18 Researchers who use patient identifying data are subject to the same requirements to protect privacy and confidentiality as a health care professional. These requirements are laid down by agencies that fund research such as the Medical Research Council or the Scottish Chief Scientist Office. Infringements are likely to lead to the loss of employment.

## CONCLUSIONS

3.19 The Data Protection Act 1998 places a legal duty on data controllers to process data fairly and lawfully, to use no more data than is necessary for the task and to retain it for only as long as it is needed.

3.20 The Human Rights Act 1998 guarantees respect for a person's private and family life. Under the terms of the Act, this right to privacy may be overridden, but only when there is a lawful reason do so.

3.21 The common law further reinforces the need to obtain patient consent before sharing information.

3.22 Professional guidelines require clinicians to ensure that patients are informed about how information about them is used and that consent requirements are met.

3.23 A substantial organisational framework for protecting the use of patient identifying information already exists in Scotland.

- 4.1 NHSScotland has a legal and moral duty to protect an individual's confidentiality. Modern healthcare systems depend however, on information from current and former patients. The existence of an effective healthcare system is in the public interest and in the interest of anyone who needs treatment. If the healthcare community were unable to make use of information from patients, it would be impossible to plan and manage services, protect and improve health. Measures to check that patients receive the correct care would be unreliable and the ability to carry out research and develop new and better treatments would be severely curtailed. It is CSAGS' view that this would be against the public interest and also the interests of all of us who at one time or another need healthcare.
- 4.2 The consequence of this blend of different interests is that NHSScotland must make sure that patient identifying information is processed fairly and confidentiality is protected but that in return, it is fair and lawful to share information from patients ***provided that high standards of confidentiality are maintained and anonymised data are used wherever possible.***
- 4.3 NHSScotland uses patient identifying information for the following purposes:
- patient care;
  - operational management;
  - clinical research; and
  - epidemiological research.

## PATIENT CARE

- 4.3.1 Patients are often treated by a team of health professionals such as nurses, doctors and occupational therapists. They may also receive social care from a local authority or voluntary agency. Some may also receive spiritual care from a minister of religion. Each member of the care team will need to have some information about the patient, so as to be able to give the correct care. If information could not be shared in this way, it would be impossible to provide effective healthcare. Presently many records are maintained on paper. This makes it very difficult to restrict the access of different professionals to the information they need to know. Even so, NHSScotland already has codes of conduct in place to prohibit inappropriate access to an individual's health records. As electronic records become more widely used, NHSScotland will have the option of developing electronic measures to ensure that each member of staff only sees that part of an individual's record which is relevant to them. However, many argue that any health professional should have unrestricted access to a patient's entire record (at least for a particular episode of care) so as to be able to decide how best to care for an individual. We hope this issue will be discussed and resolved amongst health professionals and UK health departments with a view to issuing guidance.



## OPERATIONAL MANAGEMENT

4.3.2 NHSScotland uses patient identifying information to identify the health needs of communities and to plan, provide and evaluate service provision. Examples of the way information might be used for operational management functions would be:

- assessing the health of a population so as to plan care and improvements in services;
- monitoring an outbreak of a communicable disease;
- inviting individuals to screening clinics and following up on individuals who do not attend;
- checking that a patient has received the correct quality of care; and
- checking that payments and accounts are correct.

4.3.3 Often the information used for these tasks is in a form that does not enable individuals to be identified. Sometimes however, these kinds of activity require the use of information from which individuals could be identified.

## COLLECTIONS OF DATA

4.3.4 A particular area of concern during our consultation was the use of collections of patient identifying information such as in registries. The use of information gathered together into registries has been well-established practice for many years. One of the earliest registers is the Domesday Book of 1086. Another example is the first national census, which was carried out following legislation in 1800. The term ‘registers’ often carries connotations of serious disease, legal responsibilities or vital events such as birth and death. Many registers presently in use go back several decades, sometimes several centuries. In modern times, we are now able to maintain databases or collections of data which reflect both the potential of computers and new ways of treating and caring for patients. Examples of recent registers are shown in the box below.

Type	Use/example
Preventive medicine	Immunization/screening of specific populations
Genetic Counselling	To record families at high risk (in order to be able to know the likelihood of a genetic disorder)
Specific Disease Registers	Commonly used for follow-up, treatment call up, audit, research, assessing population health needs, epidemiology eg Blind Register, Cancer Register, Diabetic Register, SMR (Scottish Morbidity Record)
Population Register	Commonly used for administering health services and for research eg Community Health Index, National Health Service Central Register and for research

Type	Use/example
Treatment Registers	eg Thyroid Disease, Joint Replacement
After Care Registers	eg Children with Special Needs
At Risk registers	eg children; occupational hazards; medical hazards; elderly or chronic sick
Skills and Resources Registers	Used for administration and planning, eg blood donors
Specific Information Registers	eg congenital defects; ophthalmic; communicable diseases
Prospective Audit and Research Studies	eg The National Child Development Study – data gathered on defined set of individuals to study change and association

4.3.5 Information is collected on people with similar characteristics so as to provide services for individuals as a group, to monitor that they are receiving the appropriate care, and to learn from that care so that services can make improvements for future patients. Generally speaking, it is in the individual's interest to be part of such a data collection, and it is in the public interest to ensure that healthcare professionals have a picture of the quality of care or state of health which people experience. However, the information will only be useful if kept accurate and this often requires the use of patient identifiable data.

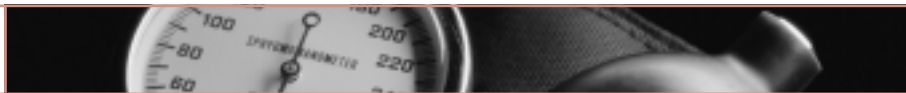
4.3.6 Collections of data are no different from registers or databases, and are integral to management of individual patient care and the administration of services. Principles of good practice are also similar to those where other uses of information are involved. It is the wish of CSAGS to ensure that any such collections are made and managed with the full knowledge of the people involved and that best practice in holding and using the information is applied.

### CLINICAL RESEARCH

4.3.7 Patient identifying information is used in trials of new treatments. It is established practice that participants are asked for explicit consent before they take part in clinical trials. The consent process will cover any use of patient identifying information.

### EPIDEMIOLOGICAL RESEARCH

4.3.8 Epidemiological studies often involve thousands of patient records but tend not to involve direct contact between a patient and a clinician nor to use named data except to link items from different sources that are then anonymised. It is expected that wherever possible people will know about such studies and that their data are likely to be included. However,



the practical difficulties in contacting large numbers of individuals can result in consent not always being sought before patient identifying information is processed.

- 4.3.9 Population-based research like this often uses large data sets (of the kind which NHSScotland collects) in order to monitor new or important diseases and to assess the effects of treatment or discover the underlying causes of disease. Examples of this are the links between smoking and cancer; between thalidomide and birth defects; or the association between leukemia in children and radiation. We depend on this kind of research in detecting new diseases and in monitoring the safety of new drugs and treatments, eg prescribing drugs to prevent thrombosis following major surgery, or for a vaccine against HIV. For most of these purposes complete data are important because opting out, even by small numbers of people, can bias the results and lead to wrong conclusions.

## Feedback from the Consultation

- 4.4 Our consultation exercise has confirmed anecdotal evidence that large numbers of health professionals are extremely concerned that involving patients in decisions about the use of their information may cause practical difficulties. They fear that some patients will withhold their data or some clinicians will be reluctant to pass on information because of concern about a legal challenge. They also anticipate delays in consultations and disruption to clinics. They make the point that the cost and impact of complying with the law is difficult to quantify but believe it would be borne by anyone who suffers from ill health.
- 4.5 A widely debated example is cancer. Presently NHSScotland has some of the best information on cancer in the world. This is because Scotland has a cancer registry which collects information on the prevalence of various types of cancer, risk factors and the effectiveness of preventions and treatments. While the registry works within established privacy and ethical frameworks, it collects and links patient identifying information from a wide range of sources without explicit consent and often without patients' knowledge. Clinicians who care for those with cancer and cancer patient representatives have made a strong case that in future, the cancer register may be unable to function effectively, unless the law is changed to allow disease registers to continuing processing patient identifying information without consent.
- 4.6 An alternative view expressed by some health professionals and individuals who participated in the consultation exercise emphasised the overriding need to ensure privacy rights are protected. Their opinion was that the attitude of many clinicians towards patients requires a fundamental change to one where a dialogue between patient and clinician, both on the care to be provided, and any use of that patient's information, is the expected norm. They thought that NHSScotland has yet to implement fully the required change of culture to

ensure that patients' rights on the uses of patient identifying information are properly recognised. They supported the idea that NHSScotland needs to ensure that its systems and procedures match the interests of patients and the public, not just those of the Service. This sentiment reflects the view that there is a broad need to change the culture of the Health Service and involve patients more in decisions about their care.

## CONCLUSIONS

- 4.7 There is a need to weigh up individual rights and claims to confidentiality against the rights and claims of individuals and the whole community to better health and to protection against threats to ill health.
- 4.8 The use of information about patients is necessary for treatment and for the operational management of NHSScotland. When used for management purposes the information can often be provided in a form that does not enable individuals to be identified.
- 4.9 Epidemiological research often relies on information derived from very large numbers of patient records. Such research rarely involves direct contact with patients.
- 4.10 Health professionals already seek informed consent before enrolling patients in clinical trials. The consent process covers any use of patient identifying information.
- 4.11 The culture of patient centred care should extend to the use of patient identifying information.
- 4.12 There is scope to review many existing information flows to confirm their compliance with the law and good practice and that they are in the interests of patients and the public.
- 4.13 There are differing views on the relative importance of time taken to discuss uses of information compared with spending time on treating the patient. It is CSAGS' view that the law requires patients to be informed; the question is the level of detail that should be given and when should explicit consent be sought.
- 4.14 There is widespread concern amongst health professionals that complying with the law and other confidentiality requirements will inhibit their ability to provide the high quality data needed to improve standards of healthcare.

- 5.1 Current NHSScotland practice and culture must change if the requirements of the law are to be met and if best practice is to take full account of policy and professional aspirations. Our review has identified the following core requirements:
- **Patients must be informed about how information about them is used.**  
Section 6 considers how this can best be done.
  - **Wherever possible, data must be anonymised to remove identifying details.**  
Section 8 considers how this may be achieved.
  - If data cannot be anonymised to an acceptable degree, **the patient has a right to object to their use**, unless there is a legal or public interest provision which overrides that right. Section 7 seeks to identify categories of data flow and to match them to appropriate consent requirements.
  - Section 10 considers whether **new legislation** should be proposed.
- 5.2 CSAGS proposes that the overall strategy should abide by the following principles:
- 5.2.1 The issue of transparency **must** be effectively addressed as most patients have little understanding of the way the healthcare community uses patient identifying information. If patients do not have a clear idea of how NHSScotland uses patient identifying information, they will be unable to give informed consent for its use.
- 5.2.2 Even when NHSScotland has patients' consent, good practice dictates that patient identifying information should only be used where there is an overwhelming case for doing so. It is always preferable to use fully anonymised information. If that is not feasible, the use of acceptably anonymised information is the alternative. Only if that proves impractical should information containing patient identifiers be used.
- 5.2.3 In the absence of legislation to the contrary, the norm should be that patient identifying information will not be used without patient consent. Consent, when sought, might be verbal or written but must always be informed and freely given.
- 5.2.4 Departures from this norm should only be possible where it can be clearly demonstrated that NHSScotland or care providers have taken reasonable measures to inform patients and where it is impracticable to gain consent or would not be the right thing to do. In situations where this arises with individual patients, eg because of continuing unconsciousness or the final stages of a terminal illness, then the clinician must be prepared to account for his or her actions.

5.2.5 CSAGS concluded that everyone in NHSScotland should be reminded of the principles of confidentiality. We proposed nine key principles in our consultation document. Having considered responses to the consultation, we have published proposed principles of confidentiality at Section 12 of this report. We think that SEHD should make sure that these are drawn to the attention of all those who work in NHSScotland.

- 6.1 As we explain in Section 3, the Data Protection Act 1998 requires data controllers to provide 'Fair Processing Information'. This means that health organisations must let patients know:
- 6.1.1 **The Identity of the 'Data Controller'**. This requirement is dealt with in detail at paragraph 3.3.
- 6.1.2 **The purposes for which the data are intended to be processed.** The detail required by patients will vary according to the situation. The aim should be to strike a reasonable balance between providing an unnecessary amount of detail and providing information in too general terms. Telling a patient visiting a GP that patient identifying information might be processed for health care purposes would be too general. On the other hand, it would be excessive for a routine visit to a GP to be used to provide a patient with a detailed explanation of all the NHSScotland systems in which patient data might be recorded.
- 6.1.3 **Any further information which is necessary, having regard to the specific circumstances in which the data are to be processed, to enable the processing in respect of the data subject to be fair.** Guidance for health organisations on how to interpret the 1998 Act is being developed by the Information Commissioner. A sensible approach might be to draw to a patient's attention, any uses or disclosures of personal data which are likely to be especially sensitive.
- 6.2 As well as providing fair processing information, CSAGS has concluded that NHSScotland needs to communicate the following concepts to patients:
- information from patients is used for a wide range of functions beyond the provision of patient care;
  - the ability to use information from patients is extremely valuable to assist with improving everybody's health and healthcare services. Increasingly patient information is used anonymously but sometimes it is necessary to identify individuals so that records can be linked;
  - even where identifying information is used, it is kept confidential;
  - in most circumstances patients can refuse to allow NHSScotland to use patient identifying information about them;
  - patients should be able to find out more about how NHSScotland uses patient identifying information.
- 6.3 When individuals come into contact with NHSScotland as patients, the Service already takes steps to let them know what to expect. Examples of this are the leaflets given to individuals when they register with a GP or go into hospital. Increasingly these leaflets include advice on the way NHSScotland uses patient identifying information. Posters explaining how such

information is used are also displayed in many NHSScotland premises. Rarely however, do the leaflets and posters advise patients of all their rights, nor do they explain whether systems are available to meet any requests for patient identifying information not to be shared. Many members of the public remain ignorant of the way the Service processes patient identifying information. It is also clear that many NHSScotland staff are unaware of these processes and are unclear of the advice to give patients. CSAGS has concluded therefore that the measures taken so far have proven to be inadequate.

6.4 There are two main ways to deal with this problem:

- a national public awareness campaign for the public and NHSScotland staff; and
- more communication with patients as and when they come into contact with NHSScotland.

### A National Public Awareness Campaign

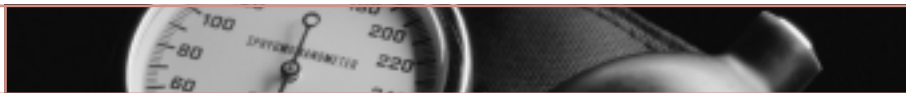
6.5 In our consultation paper we suggested that the Scottish Executive should run a public awareness campaign on how NHSScotland uses patient identifying information. The consultation exercise revealed widespread support for this from health professionals. The limited feedback we have had from members of the public also indicates that this type of initiative would be welcome.

6.6 An awareness campaign, whether a household mail drop or campaign using the press and media cannot in itself satisfy the requirement for NHSScotland data controllers to provide fair processing information. This is because:

- information would not be received by all those who use NHSScotland's services;
- it is unlikely that press notices, etc. would be able to go into the detail necessary to meet the fair processing requirement, unless they provided large amounts of information, much of which would not be relevant to many people; and
- the legal duty falls on individual data controllers and not on NHSScotland as a whole.

6.7 Whilst a national campaign will not meet fully the fair processing information requirements of the Data Protection Act, it has an important role to play in helping to make NHSScotland more transparent and accountable. It would also be an opportunity to explain why there is a need to use patient identifying information and to gain public understanding and support. This could lead to easier communication when members of the public become patients and may be asked to give their consent to certain uses of information.

6.8 SEHD is planning an awareness campaign which will inform patients of their rights. CSAGS notes that so far the progress has been slow. The Health Department has made a public commitment to an awareness campaign. CSAGS' expectation is that the campaign should start soon.



## Communication with patients as they come into contact with NHSScotland

6.9 Whilst a national awareness campaign should help, it will be for each data controller to make sure that they meet the fair processing requirements of the Data Protection Act. This means making use of the opportunities offered by contacts between NHSScotland staff and patients to provide information that is appropriate to each particular circumstance. Often the information needed will be fairly general but those who have extended contact with clinicians and carers are likely to need more specific detail about the uses of their data. We have termed these 'generic' and 'specific' in our categorisation of information and consent needs in section 7. Factors to be taken into account when deciding how much information to impart will include:

- the type of contact – eg the information needs of patients at a routine primary care appointment will be different to those receiving hospital care;
- the information needs of the patient – some individuals have no interest in how NHSScotland uses patient identifying information, some would like to know the general principles, whilst others will expect detailed advice; and
- the ability of the patient to understand. Sometimes information will need to be delivered in a particular way, eg because the individual is not an English speaker or because their vision is impaired. On other occasions the communication issues may be more complex, eg because the patient is a child.

6.10 Whilst many NHSScotland organisations have developed their own patient leaflets which explain how patient identifying information is used, our consultation exercise revealed that many NHSScotland staff would like the Scottish Executive to develop standard material which could be used to inform patients. In their view, this would avoid duplicating effort and reduce the need for individual NHSScotland organisations to develop their own material. It would also help to ensure that patients across Scotland received the same information. CSAGS understands that the Health Department is working with patient representatives to develop a leaflet which would be used throughout the Service to provide generic information to patients. We understand that this is to be made available in electronic format so that individual practices could tailor it to their own particular circumstances.

6.11 Healthcare resources are and will continue to be finite. Consequently, methods used to engage with patients must be pragmatic and practical. We recognise for instance the time constraints on GPs in their consultations with patients. Furthermore, change will have to be at a pace that can be borne by those responsible for its implementation. That said, widespread change and specified timetables will be required. And it should be borne in mind that talking to patients may be one of the most effective and valuable ways of getting information across to them. Since dialogue between NHSScotland staff and patients might

often be the best way of getting information across, CSAGS hopes that ways will be found so that staff and patients can find the time to discuss these issues if they wish.

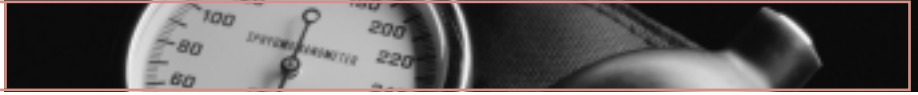
- 6.12 NHSScotland staff need to be trained and prepared for the changing relationship with patients and need to know how to deal with expressions of concern and requests for information. They also need to be aware of the requirements of law, ethics and policy and should work to agreed codes of practice. We cover staff training and awareness in section 11 of this report.

### CONCLUSIONS

- 6.13 NHSScotland staff need to be fully aware of legal, professional and organisational requirements and procedures. They should also know how to deal with enquiries from patients.
- 6.14 Most patients do not have a full understanding of the ways in which their information is used. They have a right to know more.
- 6.15 Methods used to inform patients must be practical and cost effective and as far as possible integral to their overall care.
- 6.16 A national awareness campaign would not fully meet the legal obligations of data controllers but it would help to make uses of patient identifying information open and accountable.
- 6.17 When patients come into contact with the NHSScotland, the uses to which the information gleaned from that episode might be put should be explained.
- 6.18 Patients should be informed about both specific and more general uses when using local health care services.

### RECOMMENDATIONS

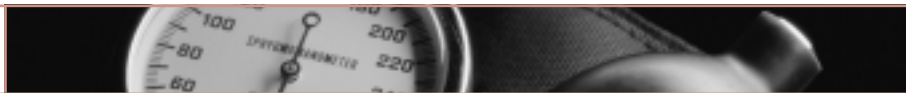
- 6.19 As a matter of urgency, SEHD should, with key partners, develop a communication strategy to inform patients of how confidential information is used. This should include working with patient and staff representatives to produce a generic information leaflet on NHSScotland uses of patient identifying information. The leaflet should be made available to support local initiatives. In the meantime appropriate locally produced leaflets and posters should continue to be encouraged.
- 6.20 The Scottish Executive should organise a national awareness campaign for staff, patients and the public.



## Final Report

- 6.21 The Scottish Executive should offer guidance to NHSScotland data controllers on how patient contacts with the NHS should be used to provide fair processing information. Depending on the type of contact, the information required may be generic or specific to a patient's circumstances.

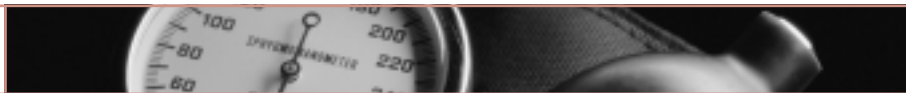
- 7.1 We explain in section 3 that NHSScotland must ensure that in certain circumstances information is only shared with the patient's consent. To be valid, that consent should be informed and freely given. In some cases, however, it should be reasonable to assume that actions imply informed consent so that explicit consent is not required. Even where explicit consent is required, it may not be necessary for a patient to sign a consent form. What is important is for all patients to be given sufficient information for them to be able to understand how patient identifying information might be used and to question and object if they wish. The use of a consent form is merely one way to provide evidence of this process.
- 7.2 Individual information flows are often difficult to categorise. In our consultation paper we concluded that it is necessary to set general principles on what the nature of consent should be in any given situation. We identified categories of information and proposed consent requirements for each. It is clear from the consultation responses that NHSScotland staff would welcome clear and specific guidance on this. However, there was considerable debate on the detail.
- 7.3 Many of those from within the NHSScotland expressed strong reservations with our views on consent requirements. Much of the concern came from respondents involved in the fields of public health and disease registries. These respondents held strong views about the importance of patient identifying information for public health, research and administrative purposes. They stressed that these functions are essential to the care of patients generally if not individually and are in the public interest. They also had major concerns about our proposal that such activities should not draw on patient identifying information unless patients had given explicit consent. Their view was that this would be impracticable because much of the data do not arise from current contacts with patients. They were also very concerned that consent refusals would pose serious risks to the provision of essential data. Similar views were expressed by respondents responsible for the planning and quality of services and for financial management and control. A further area of concern expressed by a range of respondents was the resource implication of obtaining individual consent.
- 7.4 In contrast, the limited response from patients and the two pilot focus groups indicated that patients would like to know more about such uses of their information and be more involved in decisions to use it.
- 7.5 CSAGS has carefully reviewed its proposals on consent, particularly in the light of the consultation responses. We have concluded that the separation of patient identifying information uses into the 'direct care' and 'indirect activity' categories we proposed would cause confusion and would not be helpful. It is clear that a number of functions can be said to be an essential part of the care of patients whilst not necessarily being direct hands-on



care of individuals. Many of the public health functions and local management tasks fall within this area. We are therefore proposing revised categories and these are detailed beginning at paragraph 7.7 below and illustrated on pages 30 and 31 together with the related patient information and consent requirements.

- 7.6 In relation to the consent requirements, the key in our view, lies in the effectiveness of the information given to patients. Provided it clearly explains the proposed data use and advises of opt-out possibilities and their implications both for the patient and the wider public interest, then CSAGS is now proposing that implied consent could be an acceptable minimum standard for many of the uses of patient identifying information. However, best practice remains enabling informed patients to share in decisions about the use of their data and our expectation would be that better informed consent would become the norm once improved information and recording systems are in place.
- 7.7 Our revised proposed categories are as follows:
- 7.8 **Legal Requirement.** This category remains unchanged from our original proposal. It is clear that in some circumstances, the law requires clinicians to share information irrespective of the views of a patient, eg if patients contract certain notifiable diseases. Best practice would be for the patient to be told about the sharing.
- 7.9 **Legal Defence.** The concept of processing and sharing information without consent to protect the vital interests of a patient or patients has been widely accepted. An example would be where a health professional is concerned that a child or vulnerable adult may be at risk of abuse. Professionals who have such concerns would be expected to draw them to the attention of the relevant authorities.
- 7.10 Occasionally, the sharing of patient consent can be justified as being in the interest of the public as opposed to a specific individual. An example might be the disclosure of information to the police to help in the prevention or detection of a serious crime. Both the Data Protection Act and professional standards specifically allow for information to be shared in this way.
- 7.11 Where a health professional is asked to disclose information without consent, the clinician must be prepared to justify each decision to share or withhold. It will therefore be a matter for the clinician's best judgement with decisions being taken on a case by case basis. We recognise the burden on clinicians when they are faced with such decisions and note the absence of specific guidance for them. We think it would be helpful for SEHD and professional bodies to review their guidance on this issue to ensure it is as comprehensive as possible.

- 7.12 NHSScotland Patient Care.** CSAGS has decided to restrict the term 'patient care' to mean only the use of information by those clinicians providing an individual with care. (Sometimes the care will be conducted by an independent hospital on behalf of the NHS.) Examples of using information for patient care would be referral letters and nurse hand-over notes, ie circumstances where a patient will be a participant in the care process and would almost certainly expect identifying information to be recorded and seen by all those involved in providing the care. Implied consent would be acceptable in such circumstances. CSAGS expects the proposed provision of generic information to all patients to provide for a growing understanding of such patient information uses.
- 7.13** Although clinicians must maintain good records of the treatment they provide (both in the best interests of patient care and to enable them to account for their actions if called to do so) patients would have some control over the way the record is used and a right to refuse or limit its use. This happens in some situations already. For example, records of patients using a sexually transmitted disease clinic may not have a patient's genuine name or address. Another example, more commonly found in small communities, is where a GP personally holds a patient's record so as to prevent it being seen by other practice staff who know the patient.
- 7.14 NHSScotland Operational Management and Public Health.** To address the difficulties outlined in paragraph 7.2 above, CSAGS has now introduced this terminology for a category to describe those uses of information which may not be required for the care of a specific patient but which are needed to enable NHSScotland to function. Examples of the way NHSScotland uses information for operational management purposes are at paragraph 4.3.2.
- 7.15 Multiple Uses.** This term covers information flows, which we originally proposed as an 'indirect activity' category requiring explicit consent and including disease registries, epidemiology and national data banks.
- 7.16** Many of these data flows and those categorised as 'operational management' should in our view be capable of effective anonymisation (see section 8) in which event, patient consent would not be required. For those where anonymisation is not feasible or where it cannot be introduced until technical and operational difficulties are overcome, the decision about the nature of consent to be required has been a difficult one.
- 7.17** Our initial view was that explicit consent would be the requirement, based on the ethical premise that patients have a right to know about the use of their personal health data



outwith their treatment needs and a right to withhold consent for such uses. That ideal remains best practice and our expectation is that it should become normal practice as better informed patients share in future decisions about uses of their data. However, we have found the arguments in favour of permitting implied consent for these categories persuasive, ie to safeguard valuable data for the future of services and the improvement of the health of the population.

- 7.18 We have therefore concluded that implied consent would be acceptable, provided patients are clearly informed about such uses of their data, that data controllers use only the data needed for the task and that they have a strict and monitored code of confidentiality. The right to opt-out must be integral to this although patients must be aware of the implications of this and any operational impediments in agreeing to such requests.
- 7.19 There may be circumstances when people will wish to opt-out from the sharing of their medical data, and with few exceptions they have the right to do so. The exceptions mainly concern those situations where there is a legal requirement to share information (paragraph 7.10 refers). This situation poses NHSScotland with a short-term problem and a long-term objective. In the short term it is clear that many administrative and recording systems are neither designed nor capable of coping with patient decisions to be excluded. In the long term NHSScotland should be introducing systems which can comply with patients wishes. In addition, patients will always need to be made fully aware of any possible implications for their own care and the potential effect on others from a decision to withhold their data.
- 7.20 CSAGS recognises the difficulties all this creates but is clear that the situation must be made transparent in all respects, so that all involved are aware of their rights and responsibilities as well as the current limitations of information recording systems. If, in the current situation, a wish to opt-out cannot be met, then this must be explained to and discussed with that patient. If there is no apparent solution then the local members of staff should raise the matter firstly with their Caldicott Guardian and then if necessary with the Scottish Executive Health Department for a view to be reached on the way forward.
- 7.21 **Multi-agency Care.** Modern care systems often require joint working between health and social care agencies. Whilst staff in both types of service are bound by strict arrangements for protecting confidentiality, their ways of working are necessarily different and have to meet different statutory and regulatory requirements. Our view remains that patients should be quite clear about such information sharing and be requested to consent to it explicitly. Draft protocols for inter-agency data sharing have now been published for consultation and can be found at [www.show.scot.nhs.uk/ecare/draftprotocols/](http://www.show.scot.nhs.uk/ecare/draftprotocols/). These protocols are based on the premise that explicit consent is required before personal details are shared between social care and health care organisations.

- 7.22 Research, Education and Training.** These uses of patient identifying information were not specifically identified in our consultation paper and it is clear that we should make reference to them for completeness in our categorisation proposals. It is the view of the Office of the Information Commissioner and others that identifiable data may not be shared for education, training or research without explicit patient consent. CSAGS agrees. The requirement with research is quite clear. Protocols for clinical research must provide for patients to be informed of the proposed use of their identifiable data and require their consent. NHSScotland requires researchers to obtain the approval of properly constituted ethics committees for projects involving patients and/or their data and Caldicott Guardians must authorise any release of data. Population based research utilising, or linking to data collected under implied consent, should only proceed with the appropriate approval of ethics committees, Caldicott Guardians and the Privacy Advisory Committee or its equivalent. These organisations and individuals should keep in mind evolving best practice on involving patients in these decisions.
- 7.23** The use of identifiable patient information for educational purposes such as lecturing students quite clearly requires explicit patient consent. What is more complex is the use of such information for training purposes when the training process is inextricably linked to hands on patient care. For example, at its simplest level, a nurse might make a note for hand-over but also share that as a training aid to colleagues not involved in the care of the patient concerned. If the sharing is not part of the patient care and the data cannot be anonymised, then patient consent should be obtained. What is important here is the purpose for which the information is to be used, not the relationship of the user to the patient.

### CHILDREN AND ADULTS WHO ARE UNABLE TO CONSENT

- 7.24** We recognise that there will always be situations where a patient him or herself is unable to give consent, for example, some children, adults with incapacity, and the critically ill. Guidance on the implications of the Adults with Incapacity Act already exists within the health service and from professional bodies to cover such situations and interpret the law and we do not propose to supplement that.

### CONSENT CATEGORIES

- 7.25** From paragraph 7.7 our proposed consent categories are detailed and these are set out in tabular form at pages 25 and 26. We believe that this will provide a framework to guide health service staff in assessing consent requirements for all the patient data flows they deal with and for informing patients. If the consent categories are accepted, we anticipate that SEHD will issue guidance to NHSScotland. It will then be for each NHSScotland organisation and care agency to ensure that the information flows for which they are responsible comply



with the guidance. We recognise there will be grey areas; data uses will not all fall neatly into one of our categories. Caldicott Guardians will have local responsibility for advising and guiding staff where there are difficulties and SEHD staff will continue to provide guidance on the interpretation of policy and the law. However, it seems clear that some form of adjudicating body will be needed to provide independent judgement and advice on areas of dispute which cannot be resolved. At paragraph 1.6 of this Report we refer to consideration being given to a supervisory body to review progress and it would seem logical for such a body to provide the mechanism for resolving disputes.

## CONCLUSIONS

- 7.26 Uses of patient-identifiable information can be broadly categorised to provide guidelines on information and consent requirements.
- 7.27 These categories allow for implied consent in some circumstances, require explicit consent in others and recognise specific situations where data can be used without consent.
- 7.28 Consent, whether implied or explicit must always be preceded by effective information for patients.
- 7.29 Explicit consent is best practice and should become the norm as better informed patients share in decisions about the uses of information about them.
- 7.30 There are some circumstances where, even though explicit consent would be best practice, implied consent can be accepted in the interests of the health of the population and future health needs and improvements. It is only acceptable if patients have been clearly informed about the uses to which data may be put. In addition, data controllers must only use the information needed for the task in hand and have a strict code of confidentiality in place.
- 7.31 Patients have the right to 'opt-out' but must be made aware of the implications for themselves and others and of any operational impediments

## RECOMMENDATIONS

- 7.32 SEHD should adopt the categorisation set out from paragraph 7.7 and ensure a review is undertaken of all data flows which need to use patient identifiable information to ensure compliance with the principles we have proposed.
- 7.33 SEHD, in consultation with professional bodies, should produce guidance for NHSScotland staff on the circumstances and procedures in situations where 'legal defence' can be a justification for over-riding consent requirements.

7.34 An independent body with adjudicatory powers should be set up to consider and rule on any disputes concerning consent requirements which cannot be resolved within the NHSScotland and SEHD.

## CONSENT CATEGORIES (see paragraph 7.7)

Always consider anonymisation first. If data are anonymised the need is to inform but not consent.

Release only the minimum data required.

Outlined below are the minimum requirements – best practice remains enabling informed patients to share in decisions about the release of their data.

## CONSENT NOT REQUIRED

Category	Information Need
a. <i>Legal Requirement</i> eg notifiable diseases; Abortion Act	normally <i>Inform</i> (specific)
b. <i>Legal Defence</i> eg to protect life or prevent serious injury; notification to DVLA	<i>Inform</i> where appropriate (specific)
c. <i>Anonymised</i> eg personal identifiers removed	always <i>Inform</i> (generic/specific)

## IMPLIED CONSENT ACCEPTABLE

Category	Information Need
a. <i>NHSScotland Patient Care</i> eg GP referral and hospital care	<i>Inform</i> (generic). Assume consent (but act on refusals and ensure patient aware of consequences)*.
b. <i>NHSScotland Operational Management &amp; Public Health</i>  (maintaining quality and probity) eg planning; managing; funding and auditing; where identifiable data cannot be anonymised	<i>Inform</i> (generic – but give relevant detail). Assume consent (but act on refusals)
c. <i>Multiple uses</i> (if cannot be anonymised) eg disease registries; epidemiology; national data banks	<i>Inform</i> (generic and specific). Assume consent (but act on refusals).

**Best practice is to obtain explicit consent and the expectation is that this will become the norm once better patient information and recording systems are in place.**

\*(There is a duty on clinicians to make a record but patients have a right to consent over its use)



PRIOR CONSENT REQUIRED

Category	Information Need
<p>a. <i>Multi-agency care eg sharing data with Social Work; referrals to Nursing Homes</i></p>	<p><i>Inform (specific/generic). Explicit Consent (developing protocols will provide for generic information and a wide ranging consent).</i></p>
<p>b. <i>Research using identifiable data eg clinical trials</i></p>	<p><i>Inform (specific). Explicit consent (exceptions only within provisions of Data Protection Act, section 33 and approval of Caldicott Guardians, and Ethics Committees).</i></p>
<p>c. <i>Education and Training eg identifiable patient records used to lecture medical students</i></p>	<p><i>Inform (specific/generic). Explicit Consent.</i></p>

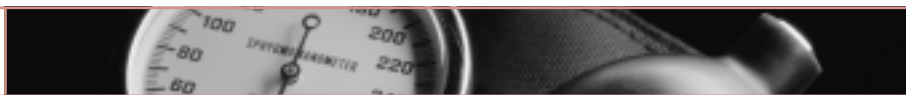
- 8.1 We explained in our initial consultation paper that one possible solution to the difficulties of gaining consent for **the sharing of personal data with third parties**, lies in anonymising data or perhaps, more accurately in making data ‘acceptably anonymous’. One aim of creating a system for anonymising data in this way is to provide researchers and similar users with a reliable source of data. The other is to protect confidentiality by ensuring that identifying data is not shared without patient consent. It is important to note that while there are no legal restrictions on the use of data that do not identify patients, **they do have a right to know when it is intended that their information will be anonymised for a range of appropriate purposes.**

## ANONYMISING ELECTRONIC DATA

- 8.2 Absolute 100% anonymity is almost impossible to achieve without a data set being reduced to one data item, rendering it of little use for many purposes. It may not however, be necessary to remove all theoretical risks of identifying an individual from a data set. CSAGS understands that data which do not contain identifying details such as name, address, date of birth and full post code may be processed lawfully without patient consent, even if a theoretical risk of a patient being identified remains.
- 8.3 The issue arose in a recent Court of Appeal<sup>1</sup> case where the Department of Health in England failed in its action to stop community pharmacists sending anonymised details of dispensed prescriptions to a company wishing to sell on the data to pharmaceutical companies for marketing purposes. The judges rejected the argument that the data were not anonymised, despite the admission from the company concerned, that ‘a remote risk that certain information of a rare kind might conceivably enable a patient to be identified’.<sup>2</sup> In other words, the data were ‘acceptably anonymous’. The case also makes clear that patients have ‘no proprietary claim’ to anonymised data and so no right to control their use.
- 8.4 ‘Acceptably anonymous’ data would reduce to tolerably low levels, the theoretical risk of identity being revealed and would ensure no risk of identification in practice. The exact data set would be a matter of consultation and judgement but might include a meaningless unique identifier (a ‘pseudonym’ not related to any other identifier) plus an appropriate part of post code, gender, year and month of birth. The GMC have identified a list of data items that prevent personal data from being anonymous, and it is understood that this list was agreed after lengthy discussions with interested parties. It says that name, address and full post code must be removed. The definition leaves open the possibility that other items could reveal identity, but it is understood that there was an intention to imply that data items like part post code and date of birth were normally acceptable.

<sup>1</sup> All England Reports (2000) pages 786-801

32 <sup>2</sup> All England Reports (2000) page 789



## A POSSIBLE ANONYMISATION PROCESS

8.5 In our consultation we proposed an anonymisation system which is set out below:

### **Step 1 – Patients give clinicians patient identifying health information.**

This is for the purpose of receiving treatment/care from NHSScotland.

### **Step 2 – Clinicians send patient identifying information required for further processing to an ‘Anonymising Service’.**

The Anonymising Service would be within NHSScotland, either at NHS board or national level, and would act on behalf of NHSScotland data controllers.

### **Step 3 – Anonymising Service substitutes patient identifiers with anonymous identifier and sends acceptably anonymised record to NHSScotland agencies holding health information databases.**

The recipient database would link the record received to previous data submissions relating to that patient by using the anonymous identifier, which would be unique and consistent for each patient. The users of the recipient database, would not be able to identify the patient.

### **Step 4 – Users, for example, researchers, gain authorisation and use acceptably anonymised health data for legitimate purposes (eg research).**

8.6 A key consideration for an anonymising service is the degree to which the ‘acceptably’ anonymised data meet the needs of the users of those data. If the users require more identifying information (most likely more post code data) then it will become easier (relatively) to identify the individual and it will be a matter for consideration when that becomes easy to the point where, in the absence of legislation to the contrary, patient consent is required.

8.7 If a generally acceptable anonymised data set is agreed which excludes data items that are of crucial importance for certain purposes (eg full post code when studying cancer clusters near power stations) it may be possible to meet these requirements by:

- encrypting the data items in question. For example the post code elements below postal district could be encrypted by the anonymisation service and given a ‘hash number’ – the same unique hash would always be produced by any given post code and so this number could be used to link full post code data together; or
- requiring the anonymising service to produce required geographical indicators from the full data set before passing on to the user.

8.8 The accountability and operation of any anonymisation service would, we suggest, have to be overseen by a Supervisory Board with a membership drawn from providers, users, and

patient representatives. The Board have to enjoy public confidence. We think it should account to Scottish Ministers.

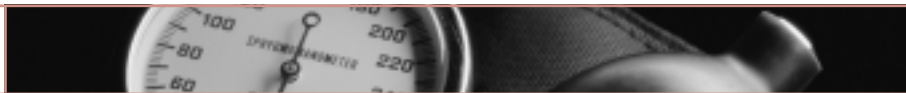
- 8.9 Many of those who responded to the consultation paper were sceptical about the creation of an anonymisation service. CSAGS recognises that the creation of an anonymisation service will be a significant challenge for NHSScotland. It is worth noting however, the view of the Information Commissioner, which is that systems like this are feasible.

## FEASIBILITY STUDY

- 8.10 As a result of CSAGS' proposals the Scottish Executive recently undertook a feasibility study on acceptable anonymisation. The report's findings are at Annex D. They indicate that it would be feasible to set up a central service to anonymise data being used on a national basis by organisations like the Common Services Agency. The study proposes that local organisations should be able to choose whether to set up their own local anonymisation service centres, applying nationally-agreed anonymisation standards, or whether to use the national anonymisation service for processing local flows. It also concludes that given the complexity of the issue, a gradual, phased implementation approach should be adopted, even if this means that every NHSScotland organisation is not able to meet our original view that 'all uses of patient identifying information should have either acceptable anonymisation or consent by the start of 2004'.

## Legislation to put 'acceptable anonymisation' on a statutory footing

- 8.11 One of the key concerns about this concept is that, under the present legislative regime, there will be no statutory definition of 'acceptably anonymised' data. Thus a healthcare professional who allows acceptably anonymised data to be used for research might still be sued by an individual who believes that though the risks of identification are very small, their confidence has been breached. This might discourage the sharing of acceptably anonymised data, with a detrimental impact on important research and educational activities.
- 8.12 One way of resolving this position would be for a law to be passed that would define 'acceptably anonymised'. The idea would be to make it clear when data are to be seen as anonymous. The argument is that if the data being processed are anonymous, common law duties of confidentiality do not apply and consent for processing is not required. Thus acceptably anonymised data could be used lawfully without consent, even though the other provisions of the Data Protection Act would have to be complied with.
- 8.13 There are two ways to come up with a definition. The first would be to set out a standard in statute. This is likely to be extremely complex. For example, it might be possible for more



detailed data to be revealed to a researcher who is under legally enforceable duties of confidentiality, than to a member of the public. The second way would be to define a process through which data must go before being considered acceptably anonymous. This would require data users to pass a series of agreed hurdles before being able to claim anonymous use of data. Examples might be to have clearance from an ethics committee, approval from the Privacy Advisory Committee and compliance with rules on publishing data.

## THE COMMUNITY HEALTH INDEX

8.14 A Community Health Index (CHI) number is allocated to every member of the public registered with a GP in Scotland. It is a ten-digit number compatible with the NHS number used in England and Wales but it differs in that it contains the individual's date of birth and gender and therefore can be said to be patient identifying. At present, use is not yet universal. SEHD policy is that in order to improve NHSScotland administration, the CHI number should be used on all correspondence such as referral letters progressively over the period to March 2003. CSAGS proposes that:

- this number is suitable for use in direct care within and between care settings (eg in clinical letters, referral and discharge letters and test results), where information such as date of birth and gender may in any case be available. SEHD's current programme of work to establish the CHI number within hospital systems for direct patient care should therefore continue; but
- the CHI number contains too much identifiable detail to be suitable for use as an identifier for data flows outside of the NHS, unless patients have consented to its use. This means patient records using CHI numbers may be shared with other caring agencies, *provided* consent has been obtained. The CHI number should not however, be contained in datasets being used for research purposes, unless its use is necessary for the project and patient consent has been obtained.

## CONCLUSIONS

8.15 Consent is not required where information has been acceptably anonymised but patients should still be informed of its use.

8.16 Even if data may be processed lawfully without consent, they should be anonymised wherever possible so as to meet the third data processing principle.

8.17 The establishment of a central anonymisation service for national uses of patient derived data is a challenge but is feasible.

8.18 Local NHS boards should be able to choose whether to use the central anonymisation service or set up their own local systems using nationally agreed standards.

- 8.19 One objective of an anonymisation service should be the creation of a supply of data which meets nationally agreed quality standards and which would be easily accessible for bona fide health researchers, etc.
- 8.20 Legislation may need to be considered to support a definition of acceptably anonymous.

### RECOMMENDATIONS

- 8.21 The Scottish Executive should develop an action plan based on the recommendations of the recent feasibility study into acceptable anonymisation. We expect this process to confirm the development of an anonymisation service is both feasible and necessary. If so, the intention should be to develop a central service for national information flows with local NHS Boards having the option to either use the national service or develop their own systems. Local systems should apply the same data standards as the central anonymisation service.
- 8.22 SEHD's programme of work to establish the CHI number within hospital systems should continue, as it is vital in supporting direct patient care.
- 8.23 The CHI number should not be used for other systems or agencies unless it is with patient consent.

- 9.1 CSAGS considered whether there were implications for the security of NHSScotland systems arising from our work on protecting patient confidentiality.
- 9.2 Extensive security policies, systems and provisions are already in place both within direct care settings and in organisations entrusted with patient identifying data for secondary analysis.
- 9.3 Nevertheless the new regulatory framework means NHSScotland must improve on existing systems. The consent and anonymisation processes described in this report will enhance the security of information used for secondary purposes.
- 9.4 Paper records are an area of relative weakness, once documents leave the records library, security and confidentiality are at risk. CSAGS thinks that systems for the protection of information in direct care settings need further development to ensure that:
- access to information within healthcare organisations is restricted to those with a need to know under clinically managed protocols;
  - such accesses are recorded electronically with audit trails that are regularly monitored;
  - the NHS as a whole learns from any breaches of security that put confidentiality at risk in an attempt to ensure they do not happen again. This will require the development of a national system to allow reports of any breaches and lessons learned to be shared.
- 9.5 CSAGS is also of the view that the Caldicott Framework needs to be revisited. It is evident that local response to its requirements (see paragraph 3.11) is patchy. The Caldicott Framework should be integrated fully into the system of clinical and corporate governance that now applies across NHSScotland, so as to make clear the responsibility of all staff within each organisation. CSAGS notes that a new Performance Assessment Framework (PAF) has been developed. CSAGS understands the PAF is the principal mechanism which NHS organisations will use for providing an annual report of performance to the Scottish Executive. CSAGS expects that next year's PAF will include performance targets for confidentiality/Caldicott issues.

## RECOMMENDATIONS

- 9.6 CSAGS considers that NHSScotland should introduce IT systems supporting direct patient care at local level that offer strong facilities for managing access to patient identifying information according to agreed clinically managed protocols. CSAGS supports SEHD's proposal that this is to be achieved progressively over a three-year period to 2004.
- 9.7 SEHD should ensure there is a system to allow reports of any breaches and lessons learned to be shared.
- 9.8 The Performance Accountability Framework should include performance targets for Confidentiality/Caldicott issue, SEHD should help NHSScotland Data Controllers to achieve them.

- 10.1 CSAGS' proposals on informing patients, seeking consent and anonymising data are intended to ensure that in future, NHSScotland complies with existing law and best practice. An additional option is to invite the Scottish Parliament to introduce new legislation which would change the current duty of confidentiality.
- 10.2 As we explain in section 3, the Schedule 1 of the Data Protection Act 1998 states that lawful processing of patient identifying information requires compliance with both statute and common law. The common law requires individuals to consent before patient identifying information is shared for some purposes. It might be possible for the Scottish Parliament, to pass a law overriding this common law requirement to have consent. If that was to happen, data could be processed lawfully without consent. This provision already exists in the case of certain notifiable diseases as explained at paragraph 3.8.
- 10.3 CSAGS consulted on this possibility in the summer of 2001. In our consultation exercise, we used the Health and Social Care Act 2001 (which now applies in England and Wales) as an example of what might be done. A statutory panel has now been set up to recommend to Westminster Ministers which uses of information are so critical to the NHS in England and Wales that there are clear grounds for overriding common law duties of confidence. Regulations made under Section 60 are to be reviewed annually. The idea is to enable patient identifying information to be used without consent until data flows are anonymised or patient consent can be obtained.
- 10.4 Other countries have adopted legislation on a permanent basis. In such cases, national parliaments have decided that certain activities are so important that they should not be subject to obligations to gain consent. Passing information to cancer registries is a common example. Often this type of legislation places strict controls on the way that information from patients can be processed.

### The Case Against Legislation

- 10.5 The prime case against legislation of this type is that it will restrict in particular circumstances an individual's right to privacy. This might have the effect of causing patients to lose faith in NHSScotland and to withhold information because of concerns that their confidentiality might be breached. There is also a possibility that permanent legislation would remove some of the current incentives to review practices with the objective of minimising the use of patient identifying information.
- 10.6 There are also technical reasons for not legislating in this way. In short, legislation will not necessarily offer a way of meeting the challenge. Regulations to allow for data to be used without consent in specific circumstances would undoubtedly miss some information flows



that are worthy of protection. Alternatively, a new disease may appear in future (as vCJD did in the 1990s) and the data required to investigate the disease may only be partial because no one could predict in advance that regulations were necessary. It is preferable therefore to have in place systems and procedures that enable information to be processed for the whole spectrum of current and potential purposes without relying on a statutory override of the individual's right to confidentiality.

## The Case For This Type of Legislation

- 10.7 Legislation may be an appropriate solution to specific problems raised by the requirement to gain consent. One much-cited example is cancer registers, but similar arguments apply to other disease registers, education and research activities which may be impractical to carry out effectively if patient consent is required.
- 10.8 The most important reason for legislating is that full population data are used for many health research and related activities. If a proportion of the population did not consent to their data being used, then all those who have an interest in the provision of effective healthcare, including clinicians, managers, researchers and MSPs would be working with partial information that would be subject to bias. Incomplete information could distort the validity of findings, especially if a small section of the population was being investigated. Furthermore, the level of bias would be difficult to predict because little would be known about those refusing consent. Data quality is variable and rarely perfect, but the NHS is continually striving to move data quality towards 100%. If patients were able to refuse consent, this could lead to a systematic and sustained drop in data quantity and quality which unlike other data quality problems, could not be improved through better practice and systems.

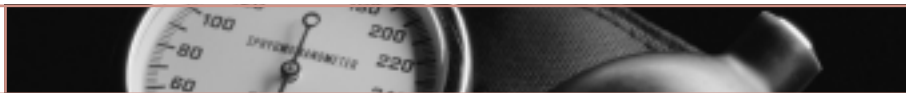
## Responses To The Consultation Exercise

- 10.9 Our consultation exercise sought views on whether the law on consent should be changed. It revealed that a large majority of NHS respondents, many of whom were from the public health and research sectors, took the view that without this type of legislation, the ability of NHSScotland to provide modern, effective and improving services would suffer. Many of these respondents were concerned that without a change to the law, the way that they used information would continue to be at risk of legal challenge. They thought that the supply of information to disease registers and other organisations would dry up as clinicians became ever more fearful of the legal implications of information sharing. Some of these respondents thought that legislation should be temporary along the lines of Section 60, so that individual clinicians and organisations were offered protection whilst new systems of consent and anonymisation could be introduced.

- 10.10 The majority of NHS respondents took the view that permanent legislation was necessary. They put forward a strong case that certain activities are so clearly in the public interest and in the interest of any individuals who may find themselves needing future treatment as to make it necessary to overrule any individual wishes to withhold potentially identifying data.
- 10.11 The views expressed by patients and their representatives were somewhat different. They suggested that what was needed was informed public support for the way NHSScotland used data so that patients would be content for their data to go forward to disease registers and other data banks. They thought that new laws might undermine the goodwill which currently exists. Their concerns were not so much about the potential for breaches of confidentiality but rather about issues of autonomy, that is the right to be told about and agree to uses of their personal data – in much the same way as understanding and agreeing to actual treatment.

## Conclusion

- 10.12 CSAGS recognises that Scotland is a world leader in the use of information derived from patient records. We also recognise the important role such information has in improving the health of the people of Scotland, supporting healthcare and enabling it to develop. We are acutely aware of the concerns that exist within the health community that the law as it presently stands is placing this in jeopardy. We are also aware that many health professionals remain unconvinced that administrative action alone will resolve the situation.
- 10.13 We have had to balance these views with those held by others, mainly from outwith the NHSScotland, who have strong reservations about legislation. In a patient-centred service, the implications of any legislation which restricts rights of individual patients and risks a loss of confidence in the service must be taken seriously.
- 10.14 CSAGS has moved some way to address the concerns of those within the Service by proposing the inclusion of many public health and disease registry information uses within the category for implied consent (section 7 refers) while steps are being taken to address requirements of patient awareness and re-design data recording systems. In section 8 we have outlined the potential for anonymising much of the sensitive data currently being used.
- 10.15 We note that the Scottish Parliament has the authority to change the law on consent. It could make these changes on a temporary or permanent basis. CSAGS has concluded that whilst steps are being taken in other ways to help NHSScotland comply with the law as it presently stands in Scotland, legislation should not be pursued, at least until changes in process we have proposed are implemented and their effectiveness monitored.



## Recommendations

- 10.16 Legislation should not be pursued to change current common law duties of confidence while the other changes recommended in this Report are being implemented.
- 10.17 The Scottish Executive should maintain contingency plans to enable legislation to be brought forward in the event that the ability of NHSScotland to change its procedures to comply with the law as it presently stands proves to be inadequate.
- 10.18 We recommend that the recommendations made in this section are reviewed in April 2004 to see whether it has proven possible to develop information systems that are both compliant with the law and that enable the supply of information in a form which makes it possible for research and other activities to continue effectively.

11.1 CSAGS' review indicated that many people in NHSScotland are unaware of the implications of the new and existing legislation for their day-to-day practice. SEHD therefore requires to promote training and develop an implementation strategy for all levels of NHSScotland. This section outlines how implementation might be achieved in practice.

## PREPARING THE GROUND

11.2 There is a need to promote a clear understanding of what is meant by terms like informed consent, explicit consent, public interest, anonymisation and acceptable anonymisation. Options for change are now being identified. Subsequent actions will have to be prioritised according to the availability of resources and to risk.

## COMMUNICATIONS WITH THE PUBLIC

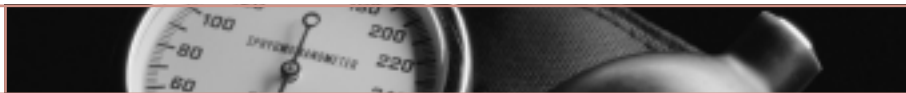
11.3 The provision of information to patients is the key to transparency and underpins valid consent and public awareness of rights. There is also a need to convey the importance of NHSScotland activity that relies upon confidential patient information and to reinforce and build on patient trust in the NHSScotland. This issue is dealt with in some detail at section 6.

## SECURING THE CONFIDENTIALITY OF PATIENT IDENTIFYING INFORMATION

11.4 Some of the change that is required to record and respect patient preferences needs new technology to be put in place and new ways of working to be developed. A better understanding of how information is used is required at a local level and appropriate security measures and privacy enhancing technologies, up to and including encryption is required. Section 9 illustrates the security implications of the changes that will be required.

## INFORMATION GOVERNANCE

11.5 The work that is needed to improve standards needs to be clearly understood, effectively resourced, and constructively managed. SEHD has already commenced a review of the implementation of the Caldicott Framework. CSAGS' view is that the Caldicott work programme needs to be strengthened and extended into partner organisations. We think that this should involve the development of a set of Key Performance Indicators for information management, confidentiality and security as part of the new Performance Assessment arrangements for NHSScotland. Since many of the required changes are cultural, a process for challenging traditional uses of confidential information is required. Barriers to increased reliance on anonymisation and acceptable anonymisation will have to be dismantled.



## COMMUNICATION WITH STAFF/CHANGE MANAGEMENT

- 11.6 A general enhancement of the duty of confidentiality and awareness of confidentiality issues by NHSScotland staff, including senior managers, would help prevent inadvertent disclosures. Examples of these include:
- staff discussing patients in public areas such as lifts or canteens;
  - patient notes being left in an area such as a corridor which is clearly visible to the public; and
  - patient identifying health information being faxed to insecure areas.
- 11.7 There is a need to ensure that staff understand the requirements of law and ethics, and that they appreciate the need for changes to systems and processes. A solution to the issues of changing NHS culture requires SEHD to take on board:
- 11.7.1 *Development of policy and guidance.* An early requirement is the development of a code of practice for NHSScotland staff who have access to confidential patient information (See section 12.) Guidance should also be developed on the role of the public interest in justifying disclosures of confidential patient information without consent (See also paragraph 7.10.)
- 11.7.2 *The provision of training and distribution of educational material.* Any campaign to inform the Scottish population about how their confidential information is used, and their rights to exert a degree of control over this, must be preceded by thorough training of staff likely to be asked questions and deal with concerns generated by the campaign. All NHSScotland staff, regardless of their role, need to be reminded of the importance of confidentiality within the NHS. A computer based training package for NHSScotland staff is now available. Training on this package will have to be supplemented by internal campaigns aimed at the whole NHSScotland workforce which should be run at regular periods. These should be timed to coincide with, or precede national campaigns aimed at the general public and patients, helping to ensure joint action. A consistent approach needs to be developed, possibly by NHS Education in Scotland, who could ensure that training aids such as the computer based package meet uniform standards and promote best practices.
- 11.7.3 The curricula of the medical and nursing schools and other venues for the training and education of health professionals also need to be modified to enhance future clinical and medical staff awareness of confidentiality issues within the NHSScotland.

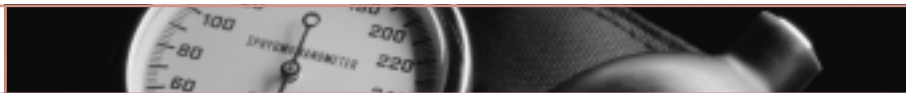
## Recommendations

- 11.8 SEHD should be required to promote training and an implementation strategy for all levels of NHSScotland. An urgent requirement is to issue a new code of practice on patient confidentiality to all those in NHSScotland.

- 12.1 As part of its deliberations, CSAGS has sought to develop some key principles which can inform discussions about patient confidentiality and which should have the following attributes:
- simplicity – to ensure they are easily remembered;
  - clarity – to make them easily understood; and
  - flexibility – to ensure that in some way they cover all possible situations and can cope with technological and other developments.
- 12.2 We propose that these principles are incorporated in revised code of practice on patient confidentiality, where they might provide easily retrieved reminders. Whilst the principles would not have a statutory basis, CSAGS recommends they are agreed with both the Information Commissioner and professional bodies prior to issue.

## P R E A M B L E

- 12.3 The generation of sensitive personal information, both in paper and electronic form, is an inevitable and essential component of the provision of health and social care.
- 12.4 It is in the individual's interest that such information should be available to those responsible for their treatment and care.
- 12.5 It is in clinicians' and carers' interests that such information should be readily available to assist them in providing appropriate and effective treatment and care.
- 12.6 It is in the public interest that information generated from individual records should be available for monitoring and audit of source material and for the planning and improvement of the population's health and social care.
- 12.7 The privacy of identifiable personal information and the autonomy of the individual concerned must be paramount and the public must have confidence in procedures to achieve this. Those who need access to personal information have a duty of confidentiality and a responsibility to ensure that patients are aware of and agree to such access. In circumstances where this cannot be achieved, any departure from the norm must be justified.
- 12.8 There will be circumstances when, in spite of being informed of the consequences, patients will wish to withhold or restrict access to their records, even though it might not be in their best interests or in the wider public health interest. Unless the law overrides personal choice in specific circumstances, eg notification of infectious diseases, the patient's wish will normally prevail.
- 12.9 All use of personal health information must be in accordance with the law.



12.10 Principles relevant to the achievement of these aims are:

**1. PATIENTS SHOULD BE THE SOURCE OF THEIR DATA**

- Seek Personal Health Information directly from patients whenever possible.

**2. INFORM PATIENTS OF THEIR RIGHTS AND RESPONSIBILITIES**

- Explain to patients what data need to be held about them and how they may be used.
- Advise patients of their rights and of opportunities for involvement in discussions about using their data.

**3. OBTAIN CONSENT**

- Observe best practice on consent requirements.
- Provide for patients to share in decisions about using their information.

**4. RECORD NO MORE INFORMATION THAN NECESSARY**

- Record only as much information as is appropriate.

**5. GET IT RIGHT**

- Make sure records are accurate, complete and up to date.

**6. KEEP IT SECURE**

- Store and send personal health information securely at all times to ensure it cannot fall into the wrong hands.

**7. SHARE WITH CARE**

- Share personal health information required for the treatment and care of patients only on a need-to-know basis.
- Share personal health information externally only with those organisations that demonstrate compliance with data protection and law and current standards of confidentiality relating to health information, or when there is a legal requirement to do so.

**8. PROVIDE FOR PATIENT ACCESS TO RECORDS**

- Respect the legal right of patients to have access to their own medical records.

**9. KNOW YOUR OBLIGATIONS**

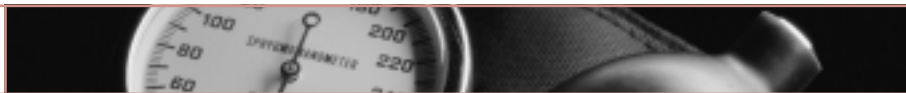
- The need for confidentiality should be a contractual obligation for all staff.
- All staff dealing with personal health information should be aware of the issues and trained to deal with them in an appropriate manner.

### CHAPTER 3 CONCLUSIONS

- The Data Protection Act 1998 places a legal duty on data controllers to process data fairly and lawfully, to use no more data than is necessary for the task and to retain it for only as long as it is needed.
- The Human Rights Act 1998 guarantees respect for a person's private and family life. Under the terms of the Act, this right to privacy may be overridden, but only when there is a lawful reason to do so.
- The common law further reinforces the need to obtain patient consent before sharing information.
- Professional guidelines require clinicians to ensure that patients are informed about how information about them is used and that consent requirements are met.
- A substantial organisational framework for protecting the use of patient identifying information already exists in Scotland.

### CHAPTER 4 CONCLUSIONS

- There is a need to weigh-up individual rights and claims to confidentiality against the rights and claims of individuals and the whole community to better health and to protection against threats to ill health.
- The use of information about patients is necessary for treatment and for the operational management of NHSScotland. When used for management purposes the information can often be provided in a form that does not enable individuals to be identified.
- Epidemiological research often relies on information derived from very large numbers of patient records. Such research rarely involves direct contact with patients.
- Health professionals already seek informed consent before enrolling patients in clinical trials. The consent process covers any use of patient identifying information.
- The culture of patient-centred care should extend to the use of patient information.
- There is scope to review many existing information flows to confirm their compliance with the law and good practice and that they are in the interests of patients and the public.
- There are differing views on the relative importance of time taken to discuss uses of information compared with spending time on treating the patient. It is CSAGS' view that the law requires patients to be informed; the question is the level of detail that should be given and when should explicit consent be sought.
- There is widespread concern amongst health professionals that complying with the law and other confidentiality requirements will inhibit their ability to provide the high quality data needed to improve standards of healthcare.



## CHAPTER 6 CONCLUSIONS

- NHSScotland staff need to be fully aware of legal, professional and organisational requirements and procedures. They should also know how to deal with enquiries from patients.
- Most patients do not have a full understanding of the ways in which their information is used. They have a right to know more.
- Methods used to inform patients must be practical and cost effective and as far as possible integral to their overall care.
- A national awareness campaign would not fully meet the legal obligations of data controllers but it would help to make uses of patient identifying information open and accountable.
- When patients come into contact with the NHSScotland, the uses to which the information gleaned from that episode might be put should be explained.
- Patients should be informed about both specific and more general uses when using local health care services.

## RECOMMENDATIONS

- The Scottish Executive should organise a national awareness campaign for staff, patients and the public.
- This work should include working with patient and staff representatives to produce a generic information leaflet on NHSScotland uses of patient identifying information for use throughout the Service.
- The Scottish Executive should offer guidance to NHSScotland data controllers on how patient contacts with the NHS should be used to provide fair processing information.

## CHAPTER 7 CONCLUSIONS

- Uses of patient identifiable information can be broadly categorised to provide guidelines on information and consent requirements.
- These categories allow for implied consent in some circumstances, require explicit consent in others and recognise specific situations where data can be used without consent.
- Consent, whether implied or explicit must always be preceded by effective information for patients.
- Explicit consent is best practice and should become the norm as better informed patients share in decisions about the uses of information about them.
- There are some circumstances where, even though explicit consent would be best practice, implied consent can be accepted in the interests of the health of the population and future

health needs and improvements. It is only acceptable if patients have been clearly informed about the uses to which data may be put. In addition, data controllers must only use the information needed for the task in hand and have a strict code of confidentiality in place.

- Patients have the right to 'opt-out' but must be made aware of the implications for themselves and others and of any operational impediments.

## RECOMMENDATIONS

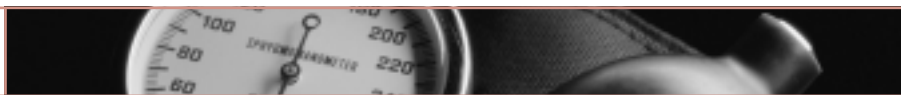
- SEHD should adopt the categorisation set out in paragraph 7.7 and ensure a review is undertaken of all data flows which need to use patient identifiable information to ensure compliance with the principles we have proposed.
- SEHD, in consultation with professional bodies, should produce guidance for NHSScotland staff on the circumstances and procedures in situations where 'legal defence' can be a justification for over-riding consent requirements.
- An independent body with adjudicatory powers should be set up to consider and rule on any disputes concerning consent requirements which cannot be resolved within the NHSScotland and SEHD.

## CHAPTER 8 CONCLUSIONS

- Consent is not required where information has been acceptably anonymised but patients should still be informed of its use.
- Even if data may be processed lawfully without consent, they should be anonymised wherever possible so as to meet the third data processing principle.
- The establishment of a central anonymisation service for national uses of patient derived data is a challenge but is feasible.
- Local NHS boards should be able to choose whether to use the central anonymisation service or set up their own local systems using nationally agreed standards.
- One objective of an anonymisation service should be the creation of a supply of data which meets nationally agreed quality standards and which would be easily accessible for bona fide health researchers, etc.
- Legislation may need to be considered to support a definition of acceptably anonymous.

## RECOMMENDATIONS

- The Scottish Executive should develop an action plan based on the recommendations of the recent feasibility study into acceptable anonymisation. We expect this process to confirm the development of an anonymisation service is both feasible and necessary. If so, the intention should be to develop a central service for national information flows with local NHS boards



having the option to either use the national service or develop their own systems. Local systems should apply the same data standards as the central anonymisation service.

- SEHD's programme of work to establish the CHI number within hospital systems should continue, as it is vital in supporting direct patient care.
- The CHI number should not be used for other systems or agencies unless it is with patient consent.

## CHAPTER 9 RECOMMENDATIONS

- CSAGS thinks that NHSScotland should introduce IT systems supporting direct patient care at a local level that offer strong facilities for managing access to patient identifying information according to agreed clinically managed protocols. CSAGS supports SEHD's proposal that this is to be achieved progressively over a three-year period to 2004.
- SEHD should ensure there is a system to allow reports of any breaches and lessons learned to be shared.
- The Performance Accountability Framework should include performance targets for Confidentiality/Caldicott issue, SEHD should help NHSScotland Data Controllers to achieve them.

## CHAPTER 10 CONCLUSIONS

- CSAGS recognises that Scotland is a world leader in the use of information derived from patient records. We also recognise the important role such information has in improving the health of the people of Scotland, supporting healthcare and enabling it to develop. We are acutely aware of the concerns that exist within the health community that the law as it presently stands is placing this in jeopardy. We are also aware that many health professionals remain unconvinced that administrative action alone will resolve the situation.
- We have had to balance these views with those held by others, mainly from outwith the NHSScotland, who have strong reservations about legislation. In a patient-centred service, the implications of any legislation which restricts rights of individual patients and risks a loss of confidence in the service must be taken seriously.
- CSAGS has moved some way to address the concerns of those within the Service by proposing the inclusion of many public health and disease registry information uses within the category for implied consent (section 7 refers) while steps are being taken to address requirements of patient awareness and re-design data recording systems. In section 8 we have outlined the potential for anonymising much of the sensitive data currently being used. In all the circumstances we remain of the view that legislation is not the favoured solution.
- We note that the Scottish Parliament has the authority to change the law on consent. It could make these changes on a temporary or permanent basis. CSAGS has concluded that

whilst steps are being taken in other ways to help NHSScotland comply with the law as it presently stands in Scotland, legislation should not be pursued, at least until changes in process we have proposed are implemented and their effectiveness monitored.

## RECOMMENDATIONS

- Legislation should not be pursued to change current common law duties of confidence while the other changes recommended in this Report are being implemented.
- The Scottish Executive should maintain contingency plans to enable legislation to be brought forward in the event that the ability of NHSScotland to change its procedures to comply with the law as it presently stands proves to be inadequate.
- We recommend that the recommendations made in this section are reviewed in April 2004 to see whether it has proven possible to develop information systems that are both compliant with the law and that enable the supply of information in a form which makes it possible for research and other activities to continue effectively.

## CHAPTER 11

### RECOMMENDATIONS

- SEHD should be required to promote training and an implementation strategy for all levels of NHSScotland. An urgent requirement is to issue a new code of practice on patient confidentiality to all those in NHSScotland.

## **CONFIDENTIALITY AND SECURITY ADVISORY GROUP FOR SCOTLAND**

### **AIM**

To provide advice on the confidentiality and security of health related information to the Scottish Executive, the Public and to Health Care Professionals.

### **TASKS**

- To set National Standards to govern the confidentiality and security of patient information within the NHS and with outside voluntary and private agencies.
- To provide guidance on patient rights and NHS requirements for information.
- To provide guidance and support to Caldicott Guardians.
- To develop a new Code of Practice on the Confidentiality of Personal Health Information for the NHSScotland and a national protocol for sharing information between health, social work, housing, etc.
- To advise on the confidentiality and security aspects of implementing the Information Management and Technology strategy.
- To input to policy making, eg development of electronic patient records.

### **COMPOSITION**

The group consists of a lay chair, Mrs Angela Macpherson, who is from a profession outwith the health sector and 19 members from a variety of professions and interest groups as follows:

Ms Carol Greer – Scottish Consumer Council  
Professor Elizabeth Russell – Professor of Social Medicine  
Dr Malcolm MacWhirter – Health Board Director of Public Health  
Mr Jim Lawrence – Health Board Medical Director  
Ms Rosemary Jamieson – Health Board Director of Information  
Mr Joe Owens – Chief Executive NHS Acute Trust  
Mr George Harper – Local Authority, Director of Housing and Social Work  
Dr Rod Muir – Information and Statistics Division, Common Services Agency  
Dr George Venters – British Medical Association  
Dr Bill Reith – Royal College of General Practitioners  
Mr Jim Wallace – Royal College of Nursing  
Mr David Arkless – Unison  
Mrs Margaret Brown – Scottish Association of Health Councils  
Dr Andrew Fraser – Deputy Chief Medical Officer, Scottish Executive Health Department  
Mr Steve Lindsay – Solicitor, Scottish Executive  
Mr Charlie Knox – Director IM & T, Scottish Executive Health Department  
Mrs Sheena Brennan – Data Protection Officer, Strathclyde Police  
Mr Neil Billing – FHS Fraud Investigation Unit  
Mrs Wendy Nganasurian – The Patients Association

### **WEBSITE**

This report is also available on the CSAGS website at <http://www.show.scot.nhs.uk/csags/>

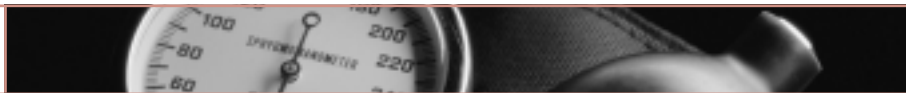
## DEFINITIONS AND GLOSSARY

### CLARIFYING DEFINITIONS

There is much confusion over the concepts of consent, anonymisation and acceptable anonymisation in both legal and healthcare circles. Part of this arises from confusion over definitions. What is required is a set of definitions onto which stakeholders can map their own definitions and uses of terms. The following table provides a set of such definitions which may need to be refined through discussion and consultation.

### GLOSSARY OF TERMS

Term	Meaning	Notes
Acceptably anonymised data	Data from which in practice the patient cannot be identified by the recipient of the information, and where the theoretical probability of the patient's identity being discovered is extremely small.	This comes close to the GMC's definition of 'anonymised data'.
Anonymised data	Data from which there is no theoretical or practical risk that a patient could be identified by the recipient of the information.	Perfect anonymisation with zero risk of identity being revealed.
Consent directions	Directions expressed by the patient indicating the terms on which their personal information may be disclosed, and what and where data may not be disclosed.	
Data disclosure	Any access to personal information given to an individual, whether it be access to a data flow or stored records, or within an organisation or across organisation boundaries.	
Express consent	Agreement which is expressed orally or in writing (except where patients cannot write or speak, when other forms of communication may be sufficient).	GMC definition.
Implied consent	Assumption that circumstances allow disclosure of information without seeking express consent.	
Informed patient consent	Express consent, plus situations where it is acceptable to rely on implied consent because the patient has been informed and has not used available mechanisms to refuse consent.	The Information Commissioner is understood to consider 'opt out' methods to be acceptable, as long as the patient is informed and has a mechanism to refuse.



Term	Meaning	Notes
Patient identifying information	A data set which may include some or all of the following: a picture of the patient, the patient's name, address, full post code or date of birth.	'Personal data' is the term used in the Data Protection Act 1998. The Act treats much health information as 'Sensitive Personal Data' – with additional protections.
'Predictable' or 'expected' data use	Circumstances where it is reasonable to assume that the patient anticipates and accepts that their data will be disclosed because, for example, they have already consented to treatment.	One example would be a referral data being sent to a hospital after the referral for treatment had been agreed with the patient.
Public interest	The interests of the community as a whole, a group within the community, or an individual other than the patient.	If judged to be sufficiently strong (such as matters of life and death), this can be grounds for acting without consent to disclosure.

GLOSSARY OF TERMS DATA PROTECTION ACT 1998

Term	Definition
Data Subject	An individual who is the subject of personal data, ie a living individual who can be identified from data, including data which relate to expressions of opinion
Data Controller	Person(s) who determines the purposes for which and manner in which any personal data (or are to be) processed
Data Processor	Person(s) (other than an employee of the Data Controller) who processes (eg obtains, holds, records or analyses) data on behalf of the Data Controller
Recipient	Person(s) to whom data are disclosed
3rd Party	Persons other than <ul style="list-style-type: none"> <li>• The data subject</li> <li>• The Data Controller</li> <li>• Employees/agents of the Data Controller/Processor</li> </ul>

## **CONCLUSIONS AND RECOMMENDATIONS FROM THE ACCEPTABLE ANONYMISATION FEASIBILITY STUDY**

### **Conclusions regarding scope of proposed anonymisation processing**

Even with informed consent, or with new legislation to protect certain activities that depend on identifying data, anonymisation processing will still be required to remove excessive patient data in order to meet the demands of the Third Principle of the Data Protection Act 1998.

It is feasible to 'acceptably anonymise' electronic patient records for legitimate 'indirect' uses.

The main components of anonymisation processing are: to strip out and/or encrypt revealing input data; to create the 'acceptably anonymised' output by linking patient records and accurately assigning a patient pseudonym; and to impose access controls on the output created.

### **Proposed standards safeguarding patient confidentiality**

There is a need to define standards on anonymisation processing and on what constitutes an 'acceptably anonymous' dataset, and for these to be applied nationally.

It is proposed here that, for a dataset to be considered 'acceptably anonymous', it must exclude patient name, address, CHI Number (or other external identifier), date of birth, full post code, and any free text fields. It could include CHI Number, full post code and date of birth in an encrypted form. It could include in unencrypted form any other relevant data about the person and their health, except for free text comment fields.

A request for 'acceptably anonymous' data must originate from an authorised user, be for a legitimate purpose, and not demand more data than are necessary to achieve that purpose.

These standards are only applicable in the controlled domain of NHSScotland, the Scottish Executive, and trusted partner organisations employing similar measures to protect confidentiality. Data would not be 'acceptably anonymous' without organisational and system protection, such as 'sacking clauses' in employment contracts, standards that prevent those with access to 'acceptably anonymised' data also having access to registers of patient-identifying data, strong system access controls, etc.

Anonymisation services should operate as data processors for data providers and data users, with their procedures stipulated in written contracts, and with matters of discretion referred to a service control authority containing representatives from organisations supplying and using data, and patients.



## Proposed limits to confidentiality safeguards and associated risks

Non-clinical staff involved in the anonymisation process require access to confidential patient-identifying data for reconciliation purposes; some legal support for this can be found in the Data Protection Act requirement that data be kept accurate, and a public interest defence could be made. However, there is a risk that this could be challenged as a breach of confidence under the common law.

In order to keep costs to realistic levels, the majority of requests for acceptably anonymised data should be 'vetted' by software and a minority by a service control authority. Inevitably, this adds slightly to the risk to that a person's identity may be revealed.

Personal data provided by a patient to one organisation could be used in an acceptably anonymised form by another organisation for a necessary purpose, even if the patient objects to this use (this position is supported by the Data Protection Act)<sup>3</sup>.

## Conclusions regarding scope of proposed anonymisation service

There should be a central anonymisation service to process national standard flows (like SMRs).

Local organisations should be able to choose whether to set up their own local anonymisation service centres, applying nationally-agreed anonymisation standards, or whether to use the national anonymisation service for processing local flows.

Simple anonymisation processing, such as control of access to local databases, should be the responsibility of local organisations rather than an anonymisation service.

## Recommendations

Legal advice should be sought on specific issues identified within this report.

The GMC and Office of the Information Commissioner should be consulted on the proposals within this report.

- CSAGS, and stakeholders in the Scottish Executive Health Department, NHSScotland and other partner organisations, should be given the opportunity to comment on proposals made in this report<sup>4</sup>.
- Having considered the legal advice provided, and feedback from stakeholders, decisions should be made on proposals within this report, and particularly whether the proposed anonymisation services should be underpinned by new legislation, and/or patient consent.

<sup>3</sup> One risk is that if the purpose is research, the Office of the Information Commissioner is likely to challenge whether research is 'necessary', even though it is listed as a necessary medical purpose within the Data Protection Act 1998. It would be costly to redesign clinical systems to implement the wishes of patients who do not want their data used for specific types of research.

<sup>4</sup> Including issues raised in section 4.5 about whether ISD processing should change to meet the requirements of the law.

- Once these decisions have been made, plans should be drawn up to design, develop and implement anonymisation services.
- Given the complexity of some aspects of these proposals, a gradual, phased implementation approach should be adopted, even if this means that every NHSScotland organisation is not able to meet the CSAGS commitment that 'all uses should have either acceptable anonymisation or consent by the start of 2004'. Action should be taken to address the potential limitations in current ISD anonymisation processing identified in section 4.5 (and particularly the routine practice of making available full SMR data to health boards), and to rollout anonymisation processing throughout NHSScotland.
- An investigation should be carried out into when and how paper records should be 'acceptably anonymised' for indirect uses.