ISBN 0-7559-0875-9

9 780755 908752

Astron B31267

NHS
SCOTLAND

NHS Code of Practice on Protecting Patient Confidentiality

SCOTTISH EXECUTIVE

YSOBEL GOURLAY
SENIOR PHARMACIST

1 INTRODUCTION

1.1 Accurate and secure personal health information is an essential part of patient health care. NHSScotland's goal is for a service that:

- protects the confidentiality of patient information;
- commands the support and confidence of public, patients and all staff, students, volunteers and contractors working in or with NHSScotland;
- complies with best practice;
- conforms with the law;
- promotes patient care, the running of care organisations, and the improvement of health and care through new knowledge; and
- works in partnership with other organisations and has clearly established and communicated protocols for sharing information.

1.2 The use of information about patients is governed by:

- statute law, e.g. the Data Protection Act 1998, the Human Rights Act 1998, the Infectious Disease (Notification) Act 1889, Adults with Incapacity (Scotland) Act 2000, the Abortion Act 1967, and many others;
- the common law in Scotland on privacy and confidentiality (which requires either consent or a legal or public interest requirement for disclosure);
- professional standards; and
- the policies and organisational standards of the Scottish Executive Health Department (SEHD) and NHSScotland, underpinned by the CSAGS report.*

*CSAGS report – Confidentiality and Security Advisory Group for Scotland, 2002

All personal health information is held under strict legal and ethical obligations of confidentiality. Information given in confidence should not be used or disclosed in a form that might identify a patient without his or her consent. There are a number of important exceptions to this rule which are described later, but patients should be involved in decisions about use of their personal health information in most circumstances.

WHAT IS PATIENT IDENTIFIABLE INFORMATION?

- the patient's name;
- the patient's address;
- the patient's full postcode;
- the patient's date of birth;
- a picture, photograph, video, audio-tape or other images of the patient
- anything else that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified; and
- the CHI (Community Health Index) number contains the patient's date of birth and a number to indicate their sex, so it should only be disclosed for health care purposes outside the NHS if the patient has been informed and agrees;

A combination of items increases the chance of patient identification.

2 REQUIREMENTS OF THE DATA PROTECTION ACT 1998

2.1 The Act provides a framework that governs the processing of information which identifies living individuals. Processing includes obtaining, recording, holding, using and disclosing information. The Act applies to all forms of records including paper, electronic and other images. It requires organisations to process fairly and lawfully any information which might enable a patient to be identified.

2.2 Patients need to be informed of the identity of the 'data controller' and the purposes to which their data will be put. The data controller is the organisation that determines how, and for what purposes, information from patients is collected. It might be a primary care practice or an NHS Board. Responsibility for complying with the 1998 Act rests with each organisation as a whole, with chief executives or primary care practitioners bearing the ultimate responsibility for the actions of their staff.

2.3 The Act requires organisations to use the MINIMUM amount of information on a **'need to know'** basis and to retain it only for as long as is needed for the purpose for which it was originally collected. Guidance on the retention periods for health records has been issued by SEHD. See www.show.scot.nhs.uk/confidentiality.

2.4 The Act also applies to partner organisations such as Local Authority Social Work Departments, housing providers, etc.

2.5 Practical guidance on the application of the Act and other relevant legal and professional guidance can be found at www.show.scot.nhs.uk/confidentiality.

3 POLICIES AND ORGANISATIONAL STANDARDS FOR NHSSCOTLAND

3.1 The SEHD aims to ensure that personal health information is kept confidential; and that patients are informed and involved in decisions about the use of their information.

3.2 The Caldicott Framework was set up in March 1999. The Framework requires each NHSScotland organisation to appoint a senior clinician such as the medical director as 'Caldicott or Information Guardian'. The Guardian's responsibilities include:

- auditing current practice and procedures;
- managing an improvement plan which is monitored through the clinical and corporate governance frameworks;
- developing protocols for inter-agency information sharing at a local level; and
- making decisions about how their organisation uses patient identifying information. For example they provide advice in relation to research studies, or disclosure in the public interest.

3.3 Each NHS Board has appointed a Data Protection Officer, from whom staff can seek advice on all aspects of data protection and confidentiality. Local Authorities also have Data Protection Officers.

3.4 It is policy that all NHSScotland employees, students, volunteers and contractors must be aware of, and respect, a patient's right to confidentiality. All employees, students, volunteers and contractors must comply with this NHSScotland Code of Practice on Protecting Patient Confidentiality. Failure to comply with the Code of Practice is a disciplinary offence. All must be aware where to seek support, further information and training, and be able to demonstrate that they are making every reasonable effort to comply with the relevant standards.

4 PROTECTING PATIENT INFORMATION

4.1 Record patient information accurately.

4.2 Keep patient information physically secure.

4.3 Follow guidance before disclosing any patient information, e.g. using established information sharing protocols.

4.4 Ensure that best practice is followed for confidentiality in respect of access to all patient information in any form, e.g. paper records, electronic data, emails, faxes, surface mail, conversations which can be overheard or phone calls.

See www.show.scot.nhs.uk/confidentiality.

4.5 Anonymise information where possible. See paragraph 8.

5 PROVIDING INFORMATION FOR PATIENTS

5.1 Patients must be informed about the need to disclose information in order to provide high quality care, e.g. between members of care teams and between different organisations for their direct health care; and other (possibly less obvious) ways that NHSScotland uses their information for such essential components of healthcare provision as planning, statistics, payment, clinical governance, clinical and financial audits.

5.2 Patients should also be informed about other uses, which provide benefits to society, e.g. health surveillance, disease registries, medical research, education and training. As far as possible information should be anonymised. Where uses are not directly associated with the health care that patients receive, staff cannot assume that patients who seek health care are content for their information to be used in these ways. Staff must consider whether patients would be surprised to learn that their information was being used in a particular way – if so, then patients are not being informed effectively.

5.3 Patients can be given information in a range of ways including leaflets, talking with them, etc., ensuring that any special language or other requirements are met appropriately.

5.4 In order to inform patients effectively, staff should:

- check that patients have received appropriate information. Suitable leaflets should be available within each NHS organisation;
- make clear to patients when information is recorded or health records are accessed;
- make clear to patients when staff are or will be disclosing information to others (who should be specified);
- check that patients are informed of the choices available

to them in respect of how their information may be used or disclosed; and the possible consequences of their decision;

- check that patients have no concerns or queries about how their information is used or disclosed;
- answer any queries personally or direct the patient to others who can answer their questions or provide other sources of information; and
- give information about and facilitate the right of patients to have access to their health records.

6 PROVIDING CHOICE TO PATIENTS ABOUT USE OF THEIR INFORMATION

6.1 Patients have different needs and values – this must be reflected in the way they are treated, including the handling of their personal information. What is very sensitive or important to one person in his or her particular circumstances may be casually discussed in public by another.

6.2 Staff must:

- obtain patient's informed consent before using their personal information in ways that do not directly contribute to, or support the delivery and planning of, their health care;
- respect and record patients' decisions to agree to or restrict the disclosure or use of information, wherever possible; and inform patients if this is not possible;
- communicate effectively with patients to ensure they understand what the implications may be if they choose to agree to, or restrict, the disclosure of their information. For example, clinicians cannot treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history; complete records need to be kept of all care provided so that neither patient safety, nor clinical responsibility for health care provision is neglected; it may be more difficult to contact patients later if a new treatment (or hazard) is discovered but their details are not on the relevant database.

7 OBTAINING CONSENT FROM PATIENTS ABOUT USE OF THEIR INFORMATION

7.1 Staff must ensure that as far as possible information is only disclosed with the patient's consent. To be valid, that consent should be informed and freely given. Consent may be verbal or written. Patients can change their choice about consent at any time.

7.2 Consent can be either implied (when a patient, having been given information about a disclosure, and opportunity to express an objection, accepts a service without voicing an objection) or explicit (when a patient actively expresses consent). It must always follow effective involvement of patients.

7.3 Explicit consent is best practice and should become the norm as better informed patients share in decisions about the uses of their information.

7.4 Always consider anonymisation if possible. If data are anonymised, it is good practice to inform the patient but consent is not needed. See paragraph 8.

7.5 Requirements for consent should be considered against each of the following criteria (for further information see www.show.scot.nhs.uk/confidentiality):

- **Legal Requirement.** In some circumstances, the law requires clinicians to disclose information irrespective of the views of a patient, e.g. if patients contract certain notifiable diseases. The Data Protection Act requires that the patient be told about the disclosure.
- **To protect patients' vital interests**, e.g. where a child or vulnerable adult may be in need of protection, at risk of death or serious harm. Professionals who have such concerns should draw them to the attention of the relevant authorities.

- **In the interest of the public.** Examples might be the production of statistics (where the individual is not identified) to assist in the planning of public services; or the disclosure of information to the police to help in the prevention or detection of a serious crime. The Data Protection Act and professional standards specifically allow for information to be disclosed in this way.
- **Children and adults who are unable to consent**. There will always be situations where a patient is unable to give consent, e.g. some children, adults with incapacity, and the critically ill. In many of these cases, particularly in the case of children, there will be someone, e.g. a parent, who is legally entitled to give consent on their behalf.

7.6 There will be occasions when staff are asked to disclose information without consent, e.g. in relation to child protection or suspected serious crime. The clinician-in-charge must be prepared to balance the considerations for and against disclosure in the interests of the patient and any third party; justify and record each decision to disclose or withhold. It will therefore be a matter for the clinician's best judgement as well as legal and professional guidance. Decisions should be taken on a case-by-case basis in the light of best available information, which may include advice from the Data Protection Officer or Caldicott or Information Guardian. Wherever possible the patient should be informed what information has been disclosed and to whom.

7.7 Patients need to be informed of any possible implications for their own care and the potential effect on others from a decision to withhold their data.

8 ANONYMISATION

8.1 Data are said to be anonymised when items such as name, address, full postcode, date of birth and any other detail that might identify a patient are removed; the data about a patient cannot be identified by the recipient of the information; and the theoretical probability of the patient's identity being discovered is extremely small.

8.2 Always consider anonymisation of data where possible.

8.3 While the Data Protection Act does not restrict the use of data that do not identify patients, patients do have a right to know when it is intended that their information will be anonymised for a range of appropriate purposes.

8.4 An anonymising service is being developed within ISD* to anonymise all national returns. NHS Boards must set up systems to ensure local data flows meet agreed national standards which are being developed with ISD.*

*ISD – Information and Statistics Division of the Common Services Agency, NHSScotland.

9 OBLIGATIONS ON INDIVIDUALS WORKING IN, OR WITH, NHSScotland

9.1 All staff, students, volunteers, and contractors must endeavour to meet the standards outlined in this code, as well as their terms of employment (or other engagement agreements). These requirements build on existing best practice. Everyone should seek to ensure that protection of patient confidentiality is built into all health care.

9.2 Staff, students, volunteers, and contractors may be constrained from meeting these standards where appropriate organisational systems and processes are not yet in place. In these circumstances the test must be whether they are working within the spirit of this code of practice and are making every reasonable effort to comply.

9.3 The need for change may apply to many existing systems and processes and it is the duty of staff to inform the Caldicott or Information Guardian of any specific problems in relation to confidentiality that are noted.

9.4 Staff working in partnership with other organisations should ensure that they are fully aware of the information sharing protocol(s) in operation.

9.5 Specific legal restrictions apply to disclosure about Sexually Transmitted Diseases (including HIV and AIDS) and Human Fertilisation and Embryology Units. Staff working in these areas need to be aware of these restrictions.

10 PATIENTS' RIGHTS OF ACCESS TO THEIR PERSONAL HEALTH RECORDS

10.1 Patients (or their parents or legally appointed representative) have the right to see and get a copy of personal health information held about them, provided (in the case of a child) they understand what this means. There may be a charge for this.

10.2 Staff should facilitate the patient's right of access. Rare exceptions include occasions where the clinician-in-charge documents that access to the record could cause serious harm to the patient's or someone else's physical or mental health; could identify someone else; or is subject to legal restrictions.

10.3 If an access request means disclosing information from, or about, a Third Party (someone other than the patient or staff involved in their care), the request may be refused unless Third Party information can be temporarily removed, or the Third Party consents to disclosure or 'it is reasonable in all the circumstances' to comply with the request without the consent of the individual.

10.4 Information needs to be provided within 40 days of a request so staff must action requests promptly.

If in doubt, staff should seek the advice of the local Data Protection Officer or consult
www.show.scot.nhs.uk/confidentiality.

Updated July 2003