NHS SCOTLAND

PROTECTING PATIENT CONFIDENTIALITY

NHSScotland Code of Practice

1 INTRODUCTION

Collecting and sharing information is essential to provide safe and effective health care. (Information from the NHSScotland Quality Strategy.) Patients entrust the NHS in Scotland with their personal information and expect you, as a member of its staff, to respect their privacy and handle their information appropriately.

All staff have an ethical and legal duty to keep patient information confidential. This code sets out the standards and practice relating to confidentiality for all staff who work in or are under contract to the NHS in Scotland. You should read this policy with your regulatory organisation's code of practice or conduct (if this applies) and your employing organisation's policies and procedures.

This booklet does not provide legal advice. You are responsible for making yourself aware of the laws and regulations which affect your role and the work you do and the place in which you work.

If you are not sure about the law or your responsibilities relating to protecting personal identifiable information, get advice from your information governance lead or, if you work in general practice, your practice manager, regulatory or professional body, or your defence organisation. (The local information governance expert for NHS boards will be the data protection officer or Caldicott guardian.)

This document replaces the 'NHS Code of Practice on Protecting Patient Confidentiality' published in 2003.

2 STAFF RESPONSIBILITIES

Patients expect that you and the NHS in Scotland will keep the information held about them confidential. This duty of confidentiality applies to:

- all staff who work for or are under contract to the NHS in Scotland, including students, volunteers, contractors and independent contractors; and
- information about patients that you come across in the course of your work.

All staff should meet the standards of practice outlined in this document, as well as those included within their terms of employment. Those who are registered health-care professionals must also keep to their own regulatory organisation's standards of conduct and practice.

If you cannot meet the standards set out in this document or those set out in your organisation's policies and procedures, you should report this, as soon as possible, to your line manager or your local information governance expert.

A serious or persistent failure to follow your organisation's policies and procedures, code of conduct or practice or guidance may lead to disciplinary action being taken against you. This could even lead to dismissal. If you are a registered health-care professional, this may also result in referring you to your professional organisation which may put your continued registration at risk. In some cases, you could even be at risk of legal proceedings.

THE MAIN POINTS

- At all times you must be aware of issues relating to confidentiality.
- Keep up to date with, and follow, the laws and codes of practice relevant to your role.
- Carry out the correct level of training in information governance which you need for your job and keep this up to date.
- Make sure that you do not compromise your professional code of conduct, or conditions of your contract of employment, by discussing work-related issues, patients, colleagues, managers, the organisation or partner organisations when using social media (such as twitter or facebook) at work or at home.
- Know and follow your organisation's policies and procedures.
- Report any possible breaches or risks of breaches of the policies to your line manager in the first instance and then contact your IG lead if you need more advice.
- Know who the information governance experts are in your organisation, and ask them for help, or ask your line manager, trade union, or professional or defence organisations.

3 DEFINITION OF CONFIDENTIALITY

THE MAIN POINTS

- There is a duty of confidentiality when one person gives information to another person in circumstances where it is reasonable to expect that the information will be kept confidential.
- This duty comes from:
  - common law – decisions made by the courts; and
  - statutes – Acts of Parliament.
- There are a number of important exceptions to this rule which we describe later in this booklet, but this applies in most circumstances.

For **information to be confidential in law** it must:

- ☐ **not** be common knowledge among lots of people, for example, the content of a discussion between a patient and a health professional; and
- ☐ be useful and not irrelevant or trivial.

The term ‘confidential information’ applies to information recorded in any format, including information that staff learn from or about individual patients or staff, even if it is not recorded. (Protective markings are used on confidential information to help you look after it properly. This is a system we and our partners use to protect information from being deliberately or accidentally released to people who are not authorised.)

THE MAIN POINTS

Individuals may be identified by any of the following:

- Name, address, full post code, date of birth.
- Community health index (CHI) number.
- Any other contact information that may allow them to be identified, for example, a phone number or email address.
- A photograph, video or audio tape or other image.
- Anything else that may be used to identify them directly or indirectly, for example, rare diseases, drug treatments or statistical analyses within a small population.

A combination of any of the above increases the chance of an individual being identified. (Information from the General Medical Council: Confidentiality: London 2009.)

4 PROTECTING INFORMATION

It is your responsibility to make sure that you follow the measures set out below to protect the confidential information you have gained privileged access to because of your role as a member of NHS staff. Your responsibility starts when you receive the information. It then continues when you use it, store it, share it with others and get rid of it. This applies to spoken and written information.

THE MAIN POINTS

- Keep accurate, relevant records.
- Record and use only the information necessary.
- Access only the information you need.
- Keep information and records physically and electronically secure and confidential (for example leave your desk tidy, take care not to be overheard when discussing cases and never discuss cases in public places. Follow your organisation's guidance when using removable devices such as laptops, smart phones and memory sticks).
- Keep your usernames and passwords secret and change your passwords regularly.
- Follow your organisation's guidance before sharing or releasing information (including checking who a person is and that they are allowed access to the information), and when sending, transporting or transferring confidential information.
- Make information anonymous where possible (**see section 11**).
- Keep and destroy information in line with local policy and national guidelines.
- **Always** report actual and possible breaches of security or confidentiality as a matter of priority.

The law says that you do not process information relating to yourself or your family, friends, colleagues, acquaintances or anyone else unless you are authorised to do so as part of your role. **Remember** that NHS organisations have electronic auditing systems in place that can identify **who** is looking at **what**, and **where** and **when** this activity took place.

See section 13 for websites that contain more detailed information about how to look after personal information safely.

5 INFORMING EFFECTIVELY AND PROVIDING CHOICE

Patients have a right to know about the information held about them, how it will be used and with whom it will be shared. It is your responsibility to make patients aware that this information may be used not only to treat and care for them, but also to support other audit or work to monitor the quality of care provided.

Patients should also be informed about other possible ways in which their information may be used which could benefit society, for example, health surveillance, disease registries, medical research, education and training. As far as possible, information should be made anonymous (see section 11). If the information is to be used in a way which is not directly associated with the care and treatment that patients receive, you cannot assume that they are happy for their information to be used in these ways. It is your responsibility to make sure that patients are aware of the wider uses of their information and to get their permission. Speak with your local IG expert if you have any concerns.

Patients can be given information in a range of ways including in leaflets, diagrams, access to online resources, and speaking with them. It is your responsibility to make sure that you provide versions in any community languages or meet other accessibility requirements. (Health Rights Information Scotland (HRIS) produce information for people of all ages who use the NHS in Scotland. Their leaflet on Confidentiality is particularly relevant.)

THE MAIN POINTS

You should:

- make clear to patients when information is or may be disclosed (shared) to others involved in their health care;
- make sure that patients are aware of the choices that are available to them on how their information may be disclosed and used;
- check with patients to make sure that they have no concerns or questions about how their information will be disclosed and may be used;
- answer any questions personally or direct patients to others who can answer their questions; and
- respect the rights of patients and help them to access their health records if they have asked to do this.

Patients have different needs and values. It is your responsibility to reflect this in the way they are treated in terms of their medical conditions, their personal and family circumstances and the way their personal information is handled. What is 'sensitive' to one person may be casually discussed in public by another. Or, something which may not appear to be sensitive, may in fact be important to an individual in their particular circumstances.

6 AGREEMENT TO DISCLOSE (RELEASE) INFORMATION

Disclosure means giving or sharing of information. Disclosure is routinely associated with asking for and getting the consent (permission) of individuals to information held about them being passed on. This consent may be spoken or written and must be fully informed and freely given. (Sections 7, 8, and 9 cover circumstances where information may be disclosed without a person's consent.)

During routine clinical care, specific consent to share information relevant to their care is not usually needed as most patients understand that their information must be shared within the healthcare team. (From the Intra NHS Information Sharing Protocol.) For example, if patients have been referred to hospital, their GP will have explained this to them and it would be clear to the patient that hospital staff need information about their condition. However, patients will usually assume that their information will only be shared with those members of the team who will be caring for them and do not expect this to be shared with others who will not be involved in their care.

If you are working with organisations other than those in the NHS, it is your responsibility to make sure that you are fully aware of the procedures for getting and recording consent, as well as the information sharing protocols.

These protocols set out a common set of rules and procedures for sharing patient information which are adopted by a number of organisations or agencies such as local authorities and the police. All NHS boards have procedures for sharing information and you should follow those which apply to your employing organisation.

If you want to use or are asked by others to provide patient identifiable information, for example, patient images such as photographs or records to help with teaching or research, it is your responsibility to make sure this is in line with the information sharing protocols, and to make sure that you remove anything that can identify patients before you release the information.

THE MAIN POINTS

- Make sure that you have the patient's permission to use information and that they understand the ways in which their information will be used.
- Make sure that patients understand exactly what they are agreeing to and how their information will be used.
- You only release the minimum information necessary.

You do not need the patient's consent to use routine information which has already been made fully anonymous. However, it is good practice to tell patients that their information may be used for these purposes. It is your responsibility to make sure that you have approval from your Caldicott Guardian before using information in these ways. See Section 11 for more information about making information anonymous.

In some cases, if patients do not give permission to share their information with other professionals, this may mean that the care and treatment provided to them may be limited. In certain rare circumstances, it may mean that it is not possible to offer them certain treatment or services.

You should tell a patient if their decision about disclosure could have implications for providing their future care or treatment. For example, if health professionals do not have access to relevant information such as a patient's past medical history, this is likely to have a negative effect on that patient's care and treatment. This is also likely to present difficulties in allowing them to be treated safely and for continuity of care to be provided.

Patients who cannot give consent

There will always be situations where some patients cannot give consent, for example, young children or adults who lack capacity. In many of these cases, particularly in the case of small children, a responsible adult, usually their parent or guardian (or other person authorised to carry out this role) who is legally entitled to speak on their behalf will be asked to give their consent. This needs to be carefully and clearly recorded.

7 DISCLOSING INFORMATION WITHOUT CONSENT

Sometimes health professionals may be asked to disclose information without consent (under section 29 of the Data Protection Act 1998) to help with serious crime investigations or to prevent abuse or serious harm to others. The following are some examples of this.

- **To protect the vital interests of a patient**, for example, if a child or vulnerable adult needs protection or is at risk of serious harm (physical, psychological, emotional, or sexual harm or death). If you have any concerns, it is your responsibility to draw these to the attention of your line manager or relevant authority as a matter of priority.
- **In the public interest**, for example, releasing information to the police to help prevent or detect a serious crime, when a serious communicable disease is passed on or to help plan public services.

The Data Protection Act 1998 and professional standards specifically allow for information to be released in this way. Each case must be judged on its own merits. As a result, it will be a matter for you as a health professional or a member of NHS staff to use your best judgement as well as getting any legal and professional guidance. Remember to consult your line manager or your local IG expert **before** you share the information.

These decisions can be complicated and should balance the considerations of releasing the information in the interests of the patient and anyone else against the need for confidentiality. Disclosure should always be proportionate and limited to the relevant details and must always be able to be justified. Where possible, you should tell the patient what information you have released, to whom and for what reason (unless this would affect the purpose, for example, an ongoing police investigation or would put you or others at serious risk of harm).

8 WHEN YOU HAVE A LEGAL DUTY TO DISCLOSE INFORMATION

In some circumstances, the law will say that you have to reveal information no matter what the views of the patient may be. This may apply if:

- someone has or is suspected to have certain infectious diseases;
- someone has been involved in a road traffic accident (to help recover any costs of treatment and tell the police);
- it is a child- or adult-protection case, where it is judged that someone is at risk of significant harm; or
- a pregnancy is terminated (telling the Chief Medical Officer).

A range of regulatory organisations and some tribunals have legal powers to access personal identifiable information relating to patients. This is as part of their duties to investigate accidents or complaints, a health professional's continued fitness to practice or to prevent and detect fraud.

Wherever possible, you should tell patients about these disclosures, unless that would undermine the purpose of the investigation, even if their consent is not needed.

It is your responsibility to always keep the level of information released to the minimum necessary.

9 DISCLOSING INFORMATION TO THE COURTS

Both the criminal and civil courts in Scotland have the power to order information to be disclosed in a number of circumstances. The basis on which confidential information is being disclosed will be fully explained in a court order. The patient concerned should be told about the order, unless this is not possible or may undermine the purpose for which the disclosure is made.

In Scotland, the system of 'precognition' (examining witnesses and others before a trial) means that a limited amount of information may be disclosed before a criminal trial. In these circumstances, the information in question will be shared with the prosecution and the defence without the patient's permission. Any information disclosed must only be about:

- the nature of any injuries that have been suffered;
- the mental state of the patient; or
- any pre-existing conditions that have been documented by an examining health-care professional and any likely causes.

NHSScotland organisations no longer routinely give the Crown the original health records of patients who are still alive for them to use in criminal proceedings. Instead, suitably authenticated copy health records can usually be used unless the patient has died.

However, the Crown may ask for the original records in certain circumstances. See Provision of medical records by NHS to courts CEL (2007) 11 for more detail.

THE MAIN POINTS

- You should release only the minimum information needed to keep to a court order and the precognition process.
- Ask for advice early on if you are not sure about what you can or cannot reveal.

10 CONFIDENTIALITY AFTER A PATIENT'S DEATH

The ethical responsibility in terms of a patient's confidentiality extends beyond their death. However, the duty of confidentiality needs to be balanced with other considerations, such as the interests of justice and the interests of people who had close or emotional ties to that person. Where appropriate, you should counsel your patients about the possibility of releasing information after death and get their views about this. This particularly applies if it is obvious that there may be some sensitivity surrounding the nature of the information in question. You also need to record these discussions in the patient's record.

Unless patients have asked for confidentiality while alive, their personal representative and any other person who may have a claim arising out of their death has a right of access to information in the patient's records, directly relevant to a claim. This applies under the terms of the Access to Health Records Act 1990. (A personal representative is defined under section 3 (1) (f) of the act as the executor or administrator of the person's estate.)

If you are not aware of any instructions from the patient, when you are considering requests for information, you should take into account the following.

THE MAIN POINTS

- Is the information likely to cause distress to, or be of benefit to, the patient's partner or family?
- Does the information also reveal information about the patient's family or anyone else?
- Is the information already public knowledge or can it be made anonymous?
- Consider the reason for releasing the information being asked for.

There are a limited number of circumstances in which you should reveal relevant information about a patient who has died. Examples are shown below.

- ☐ If a parent asks for information about the circumstances and causes of their child's death.
- ☐ If a partner, close relative or friend asks for information about the circumstances of an adult's death, and you have no reason to believe that the patient would have objected to you telling them.
- ☐ If a person has a right of access to records under the Access to Health Records Act 1990.
- ☐ On death certificates.
- ☐ For public health surveillance (in these circumstances, the information in question should be made anonymous unless this would defeat the purpose).
- ☐ To help the Procurator Fiscal with an investigation or a fatal accident inquiry.
- ☐ For national confidential inquiries or for local clinical audit purposes.

11 MAKING INFORMATION ANONYMOUS

Information is said to be anonymous when the individual cannot be reasonably identified by the person or organisation to whom the information is being disclosed. This often involves removing the name, address, full postcode and any other detail or combination of details that might support identification.

It is your responsibility to always consider making information anonymous if possible, in particular when information is being used for a purpose other than direct patient care.

While the Data Protection Act 1998 does not restrict us from using information that does not identify patients, patients do have a right to know when we will be using information in this way.

We are developing an 'anonymising' service within Information Statistics Division (ISD) of NHS National Services Scotland to make anonymous all statistical information provided to them. NHS boards should create systems to make sure that local information meets agreed national standards which are being developed with ISD.

12 LEGAL ISSUES

As a health professional or member of NHS staff, you need to be aware of the following laws relating to confidentiality.

- **The Common law of Confidentiality** is a legal obligation that comes from case law, rather than an Act of Parliament. It has been built up over many years. It is an established requirement within professional codes of conduct and practice and is contained within your NHS contract, both of which may be linked to disciplinary procedures.
- **The Data Protection Act 1998** creates a framework of rights and duties which are designed to protect the processing of personal information that identifies living individuals, for example patients' health and staff records. Processing includes holding, gathering, recording, using, disclosing and destroying information. The act also applies to all forms of media, including paper and electronic. For more information go to the Information Commissioner's Office website.
- **The Human Rights Act 1998** sets the rights and freedom that belong to people whatever their nationality and citizenship. The act contains 16 basic rights covering matters of life and death such as freedom from torture and being killed. But, they also cover rights in everyday life such as the right to respect for private and family life, their home and correspondence. In general, this means that individuals have the right to live their own life with such personal privacy as is reasonable in a democratic society, taking into account the rights and freedom of others.

- **The Computer Misuse Act 1990** protects computer programmes and data against unauthorised access or alteration. Authorised users have permission to use certain programmes and data. It is a criminal offence under the act to gain unauthorised access to computer material. This may include using another person's ID and password without authority.
- **Administrative law** NHS organisations deal with confidential patient, staff and business information to carry out specific functions. In doing so, they must act within the limits of their powers. These powers are usually set out in law and it is important that organisations are aware of the extent of their powers, in particular any restrictions that may be placed on their use or in terms of releasing confidential information. If this information is processed outside these powers, this may be unlawful and may be an offence.

13 OTHER SOURCES OF INFORMATION AND ADVICE

You can get more detailed information or advice from the following sites.

Regulatory organisations and professional organisations

- General Medical Council
- Nursing and Midwifery Council
- Health and Care Professions Council
- General Dental Council
- General Pharmaceutical Council
- British Medical Association
- Royal College of Nursing
- Royal College of Midwives
- Medical and Dental Defence Union of Scotland
- Scottish Social Services Council

UK Information Commissioner's Office

- The Information Commissioner
- Employment Code
- Good Practice Note: recording and retaining professional opinions
- Use and Disclosure of Health Data
- Data Sharing Code of Practice

Public Information

- Health Rights Information Scotland

Wider resources

- NHSS Information Governance Knowledge Network
- NHSS IG Educational Competency Framework
  (NES Dec 2011)
- Looking after information – staff awareness
  (SG Dec 2011 V2)
- Health Management Library

Scottish Government Health & Social Care Directorates

- Records Management: NHSS Code of Practice
- Information Sharing between NHSScotland and the Police
  CEL (2008) 13

APS Group Scotland
DPPAS12679 (03/12)