Code of Practice

Protecting Patients Confidentiality

The Common Law Duty of Confidentiality in practice.

Code of Practice for Health

This code sets out the Duty of Confidentiality which must be followed by all individuals who work in, are under contract to or provide services to or on behalf of NHSScotland

Date Published – 21 JULY 2023

The Scottish Government

NHS SCOTLAND

Digital Health & Care Scotland

Contents

1. Introduction

The Common Law Duty of Confidentiality, in relation to healthcare, refers to the legal obligation of professionals to protect the privacy and confidentiality of patient information. It is a fundamental principle that establishes trust between patients and healthcare providers.

Under this duty, healthcare professionals, including doctors, nurses, and other staff, are required to keep all patient information confidential and not disclose it to any unauthorized individuals or third parties. This includes any personal, sensitive, or medical information shared by the patient during the course of their treatment or consultation.

All who work within or who are engaged with the NHS in Scotland have an ethical, professional and/or contractual and legal duty to keep personal information confidential. This includes personal information relating to patients, staff and contractors and other individuals we hold personal information about.

The duty of confidentiality applies to all forms of patient information, whether written, spoken, electronic, or any other format. It extends to all aspects of healthcare, including diagnosis, treatment, discussions, and any other interactions between the healthcare provider and the patient.

Collecting and sharing information is essential to provide safe and effective health care. People entrust NHSScotland with their personal information and expect you, as a member of staff, to respect their privacy and handle their information appropriately and in compliance with the law.

This code sets the duty of confidentiality individuals who work in, are under contract to#, and/or provide services to/or on behalf of NHSScotland. This includes but is not limited to GPs, Health & Social Care Staff, volunteers, opticians, dentists, pharmacists, students and trainees.

You should read this code of practice with your regulatory organisation’s code of practice or conduct (if this applies) e.g. NMC, GMC, HPC and your NHS organisation’s policies and procedures.

Breaching your Duty of Confidentiality without valid justification can have legal and professional consequences for healthcare professionals. It is essential for healthcare providers to maintain the trust and confidence of their patients by upholding the Duty of Confidentiality and handling patient information with the utmost care and respect.

This code of practice 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 information, organisational policies or processes, get advice from your Line/Duty Manager, Data Protection Officer, your regulatory or professional body, or your defence organisation.

2. Definition of Confidential information

Confidential information refers to any sensitive or private data, knowledge or material that is not readily available to the public and is intended to be concealed to protect its value and prevent unauthorised access of disclosure.

2.1 Confidential information in the NHS

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records etc. It also includes confidential business information.

When referring to information which can be used to identify an individual includes but is not limited to:

- Name, address, full post code, date of birth.
- Community health index (CHI) number.
- Staff Payroll Number
- National Insurance 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.

3. Legal Framework

As a member of NHSScotland staff you need to be aware of the following laws relating to Data Protection and Confidentiality.

3.1 The Common law Duty of Confidentiality

This is a legal obligation that comes from case law, rather than an Act of Parliament. This duty 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.

For information to be considered confidential in Common 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.

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.

It is generally accepted that the common law allows disclosure of confidential information if:

a) The information provider has consented;
b) It is required by law, or in response to a court order; or
c) It is justified in the public interest.

These circumstances are explained later in this code.

3.2 The Caldicott Principles

The principles apply to all information collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private.

1) justify the purpose(s) for using confidential information;
2) only use it when absolutely necessary;
3) use the minimum that is required;
4) access should be on a strict need-to-know basis;
5) everyone must understand his or her responsibilities;
6) understand and comply with the law; and
7) the duty to share information can be as important as the duty to protect patient confidentiality
8) Inform patients and service users about how their confidential information is used

3.3 Data Protection Legislation

In addition to the Duty of Confidentiality we are also required to comply with data protection legislation. This requires personal information to be processed in line with the following principles.

Personal data should be:

a) processed lawfully, fairly and in a transparent manner
b) collected for specified, explicit and legitimate purposes
c) adequate, relevant and limited to what is necessary
d) accurate and where necessary kept up to date
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed
f) processed in a manner that ensures appropriate security of the personal data

Personal data should be processed lawfully, fairly and in a transparent manner. For the processing to be lawful it must rely on specified legal bases and it must not contravene any other legislative requirements.

3.3.1 The Human Rights Act 1998

This sets the rights and freedoms 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.

3.3.2 The Computer Misuse Act 1990

This 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.

3.3.3 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.

4. Roles and Responsibilities

People expect that their information will be held securely and confidentially.

As outlined below, some members of staff have a particular role in protecting personal information, some of which may be particularly sensitive in its nature.

4.1 Senior Information Risk Owner (SIRO) - an Executive Director or member of the Senior Management Board of an organisation with overall responsibility for an organisation's information risk.

4.2 Caldicott Guardian - senior person who makes sure that the personal information about those who use its services is used ethically and that confidentiality is maintained. Across healthcare, it is common practice for Directors of Public Health and other Medical Directors to perform this role.

4.3 Data Protection Officer (DPO) – an independent expert advisor on data protection regulations and practices, including information security risks.

4.4 All Staff

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

It is your responsibility to make sure that you follow the measures set out below to protect the confidential information you have gained access to because of your role within the NHS. Your responsibility starts when you receive the information. It then continues when you process it in any way including using it, storing it, sharing it with others, viewing and amending it, and disposing of it. This applies to spoken, written and electronic information, including images, videos, histology slides, etc.

You should not attempt to access or process confidential information that you are not authorised to access as part of your role, this includes attempting to access clinical records about your own health held by NHS services. In addition, you should not access clinical records of your family, friends, colleagues, neighbours, acquaintances or anyone else unless you are authorised to do so as part of your legitimate administrative or clinical duties. If you wish to access the personal information the NHS holds about you, you must follow your organisation’s process for that.

If you cannot meet the standards set out in this code of practice or those set out in your organisation’s policies and procedures, you should report this, as soon as possible, to your line manager and your NHS organisation’s Data Protection Officer.

A serious or persistent failure to follow your NHS 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.

5. Protecting confidential information

At all times you must be aware of your duty to maintain confidentiality.

You must keep up to date with, and follow, the laws and codes of practice relevant to your role.

You must carry out training in information governance which you need for your job and keep this up to date.

You should know and follow your NHS organisation's policies and procedures.

You should only access the information you need to carry out your legitimate administrative or clinical duties.

You should only use organisation approved and provided equipment and systems.

You must keep confidential information and records physically and electronically secure (for example leave your desk tidy, take care not to be overheard when discussing cases and never discuss cases in public places. Follow your NHS organisation's guidance when using mobile devices such as laptops, phones and memory sticks).

Do not share your usernames and passwords.

You must 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 in public or when using social media (such as Twitter, Facebook, Instagram, or Snapchat) at work or at home.

You must follow your NHS organisation's guidance before sharing or releasing personal information (including checking who a person is and that they are allowed access to the information), and when sending, transporting or transferring personal information. Where appropriate use anonymised information.

You should know who the Data Protection Officer and Caldicott Guardian is in your NHS organisation.

You must report any information security risks or incidents to your line manager/the appropriate on duty manager in the first instance and then ensure contact your NHS organisation's Data Protection Officer to prevent delays in reporting and appropriate responses being made.

6. Informing effectively

People have a right to know what personal information is held about them, how it will be used and with whom it will be shared. This right has been enhanced by current data protection legislation.

6.1 Your requirements

You must explain to people how their personal information is or may be disclosed (shared).

You must make sure that people are aware of the choices that may be available to them on how their information may be disclosed and used.

You must check with people to make sure that they have no concerns or questions about how their information will be disclosed and may be used.

You must ensure people are fully informed about the possible ways in which their personal information may be used and information updated as required.

Be aware - People can be informed in a range of ways including being provided with leaflets, diagrams, access to online resources, and speaking with them as part of healthcare to patient conversations. NHS Inform produce accessible information for people of all ages who use the NHS in Scotland.

7. Seeking consent to disclose information subject to Duty of Confidentiality

Disclosure means giving or sharing of information.

In line with the Common Law Duty of Confidentiality, disclosure is routinely associated with managing the expectations and ensuring the person is content with the intended disclosure of information about them.

There are circumstances where personal information may be disclosed without the person giving consent, these are described in Section 9.

When consent is required, it can be implied or explicit, spoken or written, but it must be fully informed and freely given.

During routine clinical care in the NHS, seeking 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. For example, if patients have been referred to hospital, their GP will have explained to them that to enable them to receive care and treatment the relevant hospital staff will need information about their condition.

There are situations where exceptions may apply, for instance, sharing information about clinical care provided to a detainee who is under police custody may not be shared with their registered GP without their consent.

Patients will usually assume that their personal information will only be shared with NHS or Health and Social Care Partnership staff who will are involved in the delivery and administration of their care and treatment.

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

You should tell a patient if their decision not to agree to share their personal information 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.

Be aware - There is no overarching law that governs the disclosure of confidential information. The common law and other laws that require or permit the disclosure of confidential information, including patient information, interact in complex ways and it is not possible to decide whether a use or disclosure of patient information would be lawful by considering any aspect of the law in isolation. Every situation should be dealt with individually, with all available information being considered to make a decision.

If you are unsure about the legal basis for a request for information, you should ask for clarification from the person making the request and engage senior management such as your line, or on duty, manager. =

7.1 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.

7.2 Disclosing personal information without consent

NHS Staff may require to disclose information without seeking the person's consent, this may be to help with serious crime investigations or to prevent abuse or serious harm to others. The following are some examples of this.

7.2.1 To protect the vital interests of a person: 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). For example, if someone has or is suspected to have certain infectious diseases which requires others to be protected, or someone who is unconscious or with memory loss and requires assistance.

If you have any concerns, It may assist by referring to your organisation's Public Protection Policy. Be aware, it is your responsibility to draw these to the attention of your line manager, the on duty manager or relevant authority as a matter of priority.

7.2.2 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.

7.2.3 Legal obligation
In some circumstances, the law will say that you have to disclose information no matter what the views of the person may be.

For example, this may apply if:

- 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 (informing the Chief Medical Officer).

The following legislation but not limited to may permit or influence the decision to disclose of confidential information -

- Child and Young People (Scotland) Act 2014
- Social Work (Scotland) Act 1968
- Housing (Scotland) Act 2001
- Education (Scotland) Acts 1980 & 2016
- Adult Support & Protection (Scotland) Act 2007
- Anti-Social Behaviour etc. (Scotland) Act 2004
- Health (Tobacco, Nicotine etc and Care) (Scotland) Act 2016
- Social Security (Scotland) Act 2018

7.2.4 Legal Powers of other organisations

A range of regulatory organisations, law courts and some tribunals have legal powers to access personal information relating to patients. This is as part of their duties e.g. to investigate accidents or complaints, a health professional's continued fitness to practice or to prevent and detect fraud, to assess the entitlement to a range of disability benefits. 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 for the purpose or purposes.

Each case must be judged on its own merits. As a result, it will be a matter for you as member of NHS staff to ensure you are fully informed, through getting any legal and professional guidance including from organisational policies, and by using your best judgement before you disclose any information to a third party, Remember to consult your line manager, on duty manager or your Data Protection Officer 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.

7.2.5 Disclosing personal information to the Courts and Procurator Fiscal

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 personal information is being disclosed will be fully explained in a court order. These requests must be completed within 7 days of receipt. The organisation which has raised the court order has the responsibility to notify the person concerned, unless this is not possible or may undermine the purpose for which the disclosure is made.

If you receive a court order requesting the disclosure of personal information, seek advice immediately from your Health Records Department or Data Protection Officer.

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 healthcare professional and any likely causes.

NHSScotland organisations do not provide the Crown Office and Procurator Fiscal Service (COPFS) with original health records of patients who are still alive for them to use in criminal proceedings. Instead, suitably authenticated copy of the health records are provided. If the patient is deceased, the COPFS may request the original health record.

However, COPFS may ask for the original records in certain circumstances.

7.3 Disclosure should always be appropriate, relevant and proportionate and must always be able to be justified.
Where appropriate, 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).

7.4 The main points

- You should release only the minimum information needed to keep to a court order and the precognition process.
- Be aware that original copies should never be shared.
- Ask for advice from your manager or relevant colleagues early on if you are not sure about what you can or cannot reveal. Data Protection Officers and Caldicott Guardians are expert advisors in this area with a list of contact details being found at https://www.nhsinform.scot/care-support-and-rights/health-rights/confidentiality-and-data-protection/how-the-nhs-handles-your-personal-health-information.

8. Confidentiality after a patient's death

The Common Law Duty of Confidentiality extends beyond death.

While there is no legal entitlement other than the limited circumstances covered under the Access to Health Records legislation, health professionals have always had discretion to disclose personal information to a deceased person's relatives or others when there is a clear justification, taking account of the wishes expressed in life by the deceased (e.g. if the deceased has left specific instructions not to share a diagnosis with his relatives. This should be considered, and a decision reached to disclose or not, depending on the circumstances such as harm to others).

Contact your Data Protection Officer, Caldicott Guardian or Health Records Department Manager for advice.

9. Making information anonymous

When delivering care and services directly to patients, it is usually necessary to use fully identifiable personal information. This helps ensure positive patient identification and the delivery of a safe and efficient care. However, there are some situations e.g. for service planning or evaluation, or monitoring trends, when fully identifiable personal information is not strictly necessary. In these situations, the use of anonymous information must be considered.

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

Information which has been made anonymous is not protected by the requirements of data protection law or confidentiality. However individuals are entitled to be told that their information may be made anonymous and how it will be used and disclosed. Information which has been made anonymous may still carry a risk of identification of the individual to whom it relates, and so it must always be handled with care.

9.1 Pseudonymised Information

Pseudonymisation is a security technique that can be used to reduce the ability to identify an individual from information held about them. It may involve replacing names or other identifiers which are easily attributed to individuals with, for example, a reference number. Information that has been 'pseudonymised' is not legally classified as anonymous and so the requirements of data protection law and confidentiality still apply to it.

10. Other sources of information and advice

If you require more detailed information or advice please contact your NHS organisation's Data Protection Officer, Senior Information Risk Owner or Caldicott Guardian, a list of which can be found at https://www.nhsinform.scot/care-support-and-rights/health-rights/confidentiality-and-data-protection/how-the-nhs-handles-your-personal-health-information, near the bottom of the webpage.

Further information may be available from the following organisations. Please be aware this is not an exhaustive list:

UK Information Commissioner's Office - https://ico.org.uk/
NHS Inform - https://www.nhsinform.scot/
Scottish Government - https://www.gov.scot/
Regulatory organisations and professional organisations:

- General Medical Council - https://www.gmc-uk.org/
- Nursing and Midwifery Council - https://www.nmc.org.uk/
- Health and Care Professions Council - https://www.hcpc-uk.org/
- General Dental Council - https://www.gdc-uk.org/
- General Pharmaceutical Council - https://www.pharmacyregulation.org/
- British Medical Association - https://www.bma.org.uk/
- Royal College of Nursing - https://www.rcn.org.uk/
- Royal College of Midwives - https://www.rcm.org.uk/
- Medical and Dental Defence Union of Scotland - https://www.mddus.com/
- Scottish Social Services Council - https://www.sssc.uk.com/