CONFIDENTIALITY POLICY

Medic Now
Confidentiality Policy

Introduction

All healthcare service providers have an ethical, legal, and contractual duty to protect patient confidentiality. Information sharing can help to improve the quality of care and treatment, but it must be governed by the legal and ethical framework that protects the interests of patients.

Patients entrust the healthcare providers with their personal information and expect us to respect their privacy and handle their information appropriately. Everyone should seek to ensure that protection of patient confidentiality on collecting and sharing information is built into all healthcare to provide safe and effective care.

Scope

Both employed and self-employed workers, students, volunteers, and contractors must be aware of and respect a patient's right to confidentiality and must comply with this premise to protect patient and other workers confidentiality, which is built on best practice.

All workers that share information are obliged to adhere to this policy and guidelines. Managers at all levels are responsible for ensuring that the workers for whom they are responsible are aware of, and adhere to, this policy. The service is also responsible for ensuring workers are updated regarding any changes in this policy.

Definitions

Personal confidential data: information that relates to an identified or identifiable individual. This data should not be processed without a clear legal basis. Personal confidential data should only be disclosed with consent or under statute, and any disclosure must always be limited and accompanied by a contractual agreement that mitigates the risk of misuse and inappropriate disclosure. The contractual agreement needs to set out, as a minimum, the legal basis for the data flow, the purposes to which the data can be put, the safeguards that should be in place to protect data and how the public are informed about these.

Patient identifiable information: 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. Patients should be involved in decisions about the use of their personal health information in most circumstances. Patient identifiable information includes:

- Name
- Address
- Full post code
- Date of birth
- NHS number
- National Insurance Number
- Pictures, photographs, videos, audio¬tapes or other images of the patient, as even a visual image (e.g., photograph) is sufficient to identify an individual

Any data or combination of and other information, which can indirectly identify the person, will also fall into this definition.

Non-person-identifiable information: can be classed as confidential, such as confidential business information (e.g., financial reports and commercially sensitive information, e.g., contracts, trade secrets and procurement information) which should also be treated with the same degree of care.

Medic Now
Confidentiality Policy

Special categories of personal information: previously known as 'sensitive' personal data, defined by the Data Protection Act 2018 as refers to personal information about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Processing of genetic data
- Biometric data (for the purpose of uniquely identifying a natural person)
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Principles

A. All workers must ensure that the following principles are adhered to:
   - » Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of
   - » Access to person-identifiable or confidential information must be on a need-to-know basis
   - » Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required
   - » Recipients of disclosed information must respect that it is given to them in confidence
   - » If the decision is taken to disclose information, that decision must be justified and documented
   - » Any concerns about disclosure of information must be discussed with the Line Manager

B. Organisations are responsible for protecting all the information it holds and must always be able to justify any decision to share information

C. Person-identifiable information, wherever possible, must be made anonymous by removing as many identifiers as possible whilst not unduly compromising the utility of the data

D. Access to rooms and offices where terminals are present or person identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties

E. All workers should clear their desks at the end of each day. In particular they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked

F. Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Any document containing confidential information must not be left lying around but be filed and locked away when not in use

The eight Caldicott principles

Good information sharing is essential for providing safe and effective care. There are also important uses of information for purposes other than individual care, which contribute to the overall delivery of health and social care or serve wider public interests.

Medic Now
Confidentiality Policy

These principles apply to the use of confidential information within health and social care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

1. Justify the purpose for using confidential information
2. Use confidential information only when it is necessary
3. Use the minimum necessary confidential information
4. Access to confidential information should be on a strict need-to-know basis
5. Everyone with access to confidential information should be aware of their responsibilities
6. Comply with the law
7. The duty to share information for individual care is as important as the duty to protect patient confidentiality
8. Inform patients and service users about how their confidential information is used

Working away from the office/clinical environment

There will be times when workers may need to work from another location or whilst travelling. This means that these workers may need to carry health information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents.

- Taking home/ removing paper documents that contain person-identifiable or confidential information from organisation's premises is discouraged
- To ensure safety of confidential information workers must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations
- When working away from the organisation's locations workers must ensure that their working practice complies with local policies and procedures
- Workers must minimise the amount of person-identifiable information that is taken away from organisation's premises
- If workers do need to carry person-identifiable or confidential information they must ensure the following:
  - » Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of the organisation's buildings
  - » Confidential information is kept out of sight whilst being transported
- If workers do need to take person-identifiable or confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/ colleagues must not be able to see the content or have any access to the information
- Workers must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Workers must not use or store person identifiable or confidential information on a privately-owned computer or device

Carelessness

All workers have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally.

Medic Now
Confidentiality Policy

Workers may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents
- Leave a computer terminal logged on to a system where personidentifiableor confidential information can be accessed, unattended

Steps must be taken to ensure physical safety and security of person identifiable or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Workers must not use someone else's password to gain access to information.

Abuse of privilege

It is strictly forbidden for workers to knowingly browse, search for or look at any personal or confidential information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

When dealing with person-identifiable or confidential information of any nature, workers must be aware of their personal responsibility, and abide by local policies.

If workers have concerns about this issue they should discuss it with their Line Manager onsite or can be raised to the Clinical Advisory Team: *CASupport@yourworld.com*

Confidentiality dos and don'ts

Dos

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of Medic Now
- If working at a desk, do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password protected mode, if you leave your desk for any length of time
- Do ensure that you cannot be overheard when discussing confidential matters
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know
- Do share only the minimum information necessary
- Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk
- Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken
- Do report any actual or suspected breaches of confidentiality
- Do participate in induction, training and awareness raising sessions

Medic Now
Confidentiality Policy

Don'ts

- Don't share passwords or leave them lying around for others to see
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary

Reporting a breach

If a worker becomes aware of a personal data breach, they should follow the local organisation's procedure for reporting a data breach. Usually, this is in the Information Governance policy, and will require the worker to report the incident via the incident reporting process in the organisation or tell the Data Protection Officer (DPO) if they are unsure what to do.

Workers should report a data breach as soon as they become aware of it via the local organisation's incident reporting process. The report should set out what has happened and any steps you have taken in response to the breach. For example, "email containing the name, DOB and NHS number of a patient sent to the wrong Jane Smith on 5 March. Recalled the email and asked the recipient to delete it and they have confirmed this." Workers should contribute to any relevant investigation carried out.

If a worker are not sure if a breach has occurred, they should still report the breach via the local organisation's incident reporting system. Workers should also consider reporting "near miss" data breaches. A near miss is where a breach could have occurred if an incident had developed or been left. An example is leaving patient records unsecured in a main hospital corridor used by the public. Reporting near misses helps the organisation consider changes to ensure that information is kept secure.

What should be reported

The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords
- Unauthorised access to NHS/Health systems either by staff or a third part
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act and NHS Code of Confidentiality
- Sending person-identifiable or confidential information in a way that breaches confidentiality
- Leaving person-identifiable or confidential information lying around in public area
- Theft or loss of person-identifiable or confidential information
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing off person identifiable information in ordinary waste paper bin

Medic Now
Confidentiality Policy

Further information

- *The Eight Caldicott Principles*
- *Human Rights Act 1998*
- *Computer Misuse Act 1990*
- *NHS Confidentiality Code of Practice*
- *Personal Data Breaches*