Rose
MEDICAL PRACTICE
140 Fitzwilliam Street
Huddersfield
HD1 5PU

CONFIDENTIALITY POLICY

Written By: Sally Oldbury
Reviewed: Annually
Due for Review: Feb 2025
Version: 14

Purpose

The purpose of this Policy is to ensure that everyone working within the practice is aware of his or her responsibilities when using confidential information. The principle underpinning this Policy is that no employee shall misuse any information or allow others to do so.

The Policy has been written to support staff in compliance with the following legal requirements and best practice guidance:-

- Data Protection Act 2018 (updated for GDPR)
- Human Right Act 1998
- Common Law of Confidentiality
- The Caldicott Report 1997
- The NHS Confidentiality Code of Conduct
- Computer Misuse Act 1990

What is Confidentiality?

We hear the words "confidential" or "confidentiality" being used all the time within the NHS, but do we actually understand what it means, in relation to our own areas of work?

Confidentiality is the responsibility of **all** staff members. Anyone employed by, or on behalf of the NHS has a clause in his or her contract of employment, which states that the employee has a "common law duty to uphold standards of confidentiality".

What is confidential information?

There are a few simple guidelines that may help us to fulfil our obligations towards maintaining standards of confidentiality: -

- Firstly, any paper documentation or spreadsheets, databases, electronic "Microsoft Word" documents, etc, you hold which may contain the names of individuals (patients or staff members) should be classified as "confidential". Confidential information should be available only to those members of staff, who have a justified reason to view it, and should be used and stored within a private and secure environment.

- Secondly, we are all in a position of trust in relation to the information we keep. We must treat **any** information given to us in confidence as if it were our own. Would you want your bank statements to become publicly known, or details of your own health record available to all? Would you be pleased if you overheard a colleague discussing private details from your personnel file?

- And last but not least, if you don't have a justified "need to know" as part of your role, then you shouldn't access any information e.g. viewing patient information systems to check your neighbours birthday or reading through the medical notes of an old school friend are entirely

inappropriate actions and could lead to disciplinary proceedings being taken against you.

The types of information to which confidentiality applies are many and varied, but these could be broadly grouped as follows:

- ✓ **Information relating to patients**: e.g. Medical Records, appointment lists, letters to patients, complaints letters or information held on the Clinical System (EMIS)
- ✓ **Information relating to staff members**: e.g. Personnel records, wage slips, letters to individual staff members, documents or reports relating to individual disciplinary/grievance procedures
- ✓ **Financial information:** e.g. invoices, travel claims, reimbursements, statements
- ✓ **Organisation sensitive information**: e.g. tendered bids, information relating to potential service changes (prior to public consultation procedures), closure of buildings prior to consultation procedures
- ✓ **Any information you receive in confidence**

Further Help?

If you are requested to pass on any of the types of information listed above, and you are unsure whether or not it would be appropriate to do so, check with the Practice Manager.

Who does this apply to?

This Policy applies to all personal identifiable information, whether written, computerised, visual or on audio record, or simply held in the memory of a member of staff. It applies equally to staff on permanent, temporary or voluntary placement.

Health care professionals and the staff that support them hold information about people that may be private and sensitive. Patient information is collected to provide care and treatment to individuals and generally must not be used for other purposes without the individual's knowledge and permission. In the same way information about staff, which is processed for the purpose of their employment should be treated as confidential. Confidentiality should only be breached in exceptional circumstances and with appropriate justification.

Main Principles?

All staff should ensure that the following principles are practiced:

- When you are responsible for confidential information you must make sure that the information is effectively protected against improper disclosure when it is received, stored, transmitted or disposed of;
- Confidential information must only be accessed by you if it is appropriate to the job that you are employed to undertake;

- Every effort should be made to ensure that patients understand how information about them will be used before they actually supply any confidential information;
- When patients give consent to disclosure of information about them, you must make sure they understand what will be disclosed, the reasons for disclosure and the likely consequence/s;
- You must make sure that patients understand when information about them is likely to be disclosed to others involved in their health care, and that they have the opportunity to withhold permission;
- If you are required to disclose information outside the team that could have personal consequences for patients or clients, you must obtain their consent. If the patient or client withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:
    - ✓ they can be justified in the public interest (usually where disclosure is essential to protect the patient or client or someone else from the risk of significant harm)
    - ✓ they are required by law or by order of a court

- If you are required to disclose confidential information you should release only as much information as is necessary for the purpose;
- You must make sure that the persons to whom you disclose information understand that it is given to them in confidence which they must respect;
- If you decide to disclose confidential information, you must be prepared to explain and justify your decision. If you have any doubts discuss them with your line manager.

The Computer Misuse Act 1990 established three prosecutable offences against unauthorised access to any software or data held on any computer. The offences are:

- *Unauthorised Access to Computer Material*
- *Unauthorised Access with intent to commit or facilitate the commission of further offences*
- *Unauthorised Modification of Computer Material*

Shred All Policy

This Practice adopted a Shred-All Policy in 2015 in order to protect patient identifiable information or practice data which may be confidential. A Shred-All (or "better safe than sorry") Policy means staff don't have to think about whether it contains any confidential material or not, if its paper or card it goes in the secure shredding bin.

- ✓ Strengthens information privacy and confidentiality
- ✓ Simplifies document disposal for everyone
- ✓ Employees no longer need to decide what information is or isn't confidential
- ✓ Reduces the risk of information breaches
- ✓ Improves compliance with privacy rules and regulations
- ✓ Better protects proprietary, customer and other business information

Please remember;

- All office paper and documents must be deposited into the security containers located in each area
- You don't need to think is this confidential or not - allows for fewer errors.
- Conveniently placed security containers will allow for easy access for all employees (1st floor landing, GP's room, reception office & PM's office).
- Please don't put plastic bags, compete 3-ring binders or wrappings into the bin
- Paper clips, rubber bands, staples are fine
- Don't allow a shredding pile to develop over the course of the day, ensure once dealt with that each item is placed in the shredding bin.
- Please contact your manager with any questions or requests.

Breach of confidentiality

If you breach confidentiality or allow it to be breached by your actions this will be regarded as a disciplinary matter and you will be suspended while a full investigation takes place. You may also be open to civil prosecution by the patient or patients involved. Therefore it is in your best interest to ensure that confidential information is treated with the necessary respect.

Under GDPR any breach of confidentiality information must be reported to the ICO within 72 hours of recognition that a breach has occurred. Where this does not result in any harm to the patients' rights or freedoms this may be downgraded. Please ensure that any breach or near miss is reported to the Practice Manager so that it can be investigated and reported onwards if necessary.

See also Confidentiality NHS Code of Practice Nov 2003 (attached)