Didcot Health Centre
Confidentiality policy (2)

Table of contents

1 Introduction

1.1 Policy statement

All staff working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not purely a requirement of their contractual responsibilities; it is also a requirement within the common law duty of confidence, and the NHS Care Record Guarantee. The latter is produced to assure patients regarding the use of their information.[1]

1.2 Status

The practice aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have in regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are contractual and therefore form part of your contract of employment. Employees will be consulted on any modifications or change to the document's status.

1.3 Training and support

The practice will provide guidance and support to help those to whom it applies understand their rights and responsibilities under this policy. Additional support will be provided to managers and supervisors to enable them to deal more effectively with matters arising from this policy.

2 Scope

2.1 Who it applies to

This document applies to all employees of the practice. Other individuals performing functions in relation to the practice, such as agency workers, locums and contractors, are encouraged to use it.

2.2 Why and how it applies to them

This policy outlines the principles that are to be adhered to by all staff at Didcot Health Centre to ensure that person-identifiable information or confidential information is protected appropriately.

[1] NHS(E) Confidentiality Policy

3 Definition of terms

3.1 Care Quality Commission

The Care Quality Commission (CQC) is the independent regulator of health and adult social care in England. The CQC makes sure that health and social care services provide people with safe, effective, compassionate, high-quality care and encourage services to improve.[2]

3.2 Confidentiality

Confidentiality is the principle of keeping secure and secret from others, information given by or about an individual in the course of a professional relationship.[3]

3.3 Person-identifiable information

This is information that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, etc.[4]

3.4 British Medical Association

The British Medical Association (BMA) is the trade union and professional body for doctors in the United Kingdom.[5]

4 Associated policies

4.1 Practice privacy notice

The Practice Privacy Notice explains to patients the ways in which the practice gathers, uses, discloses and manages a patient's data. It fulfils a legal requirement to protect a patient's privacy.

4.2 Caldicott policy

The practice Caldicott Policy outlines the seven Caldicott principles and how they are to be applied in practice.

[2] CQC Who we are
[3] BMJ - Confidentiality definition
[4] NHS(E) Confidentiality Policy
[5] BMA

4.3 General Data Protection Regulation

The practice GDPR Policy reflects the aim of the GDPR, which is to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way in which organisations across the region approach data privacy.[6]

4.4 Information-sharing agreement

The Practice Information-Sharing Agreement Policy outlines how the practice conforms to the NHS(E) Information Sharing Policy in relation to the sharing of information with NHS and non-NHS organisations.

5 Confidentiality in practice

5.1 NHS Code of Practice 2003

All staff at Didcot Health Centre must to adhere to the principles of confidentiality outlined in the Code: [7]

- 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 the 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 the disclosure of information must be discussed with your line manager or the Practice Manager.

5.2 Good practice

The following actions at Didcot Health Centre will be undertaken to ensure that confidentiality is maintained:

- Person-identifiable information will be anonymised so far as is reasonably practicable, whilst being mindful of not compromising the data
- Access to consulting rooms, administrative areas and record-storage areas will be restricted
- A clear-desk policy is in operation at all times, and is applicable to all staff
- All office IT equipment (except servers) is shut down at the end of the working day

[6] EU GDPR overview

[7] NHS(E) Confidentiality Policy

- Where clinical computers are left on to allow GP remote access, they are logged out and in a locked room
- Confidential waste is shredded and disposed of appropriately

Furthermore, staff will not:

- Talk about patients or confidential information in areas where they may be overheard
- Leave computers or other equipment logged on when they are not in attendance
- Leave smart cards in unattended computers
- Leave any patient confidential information in unsecured areas at any time.

5.3 Confidentiality breach

Any breach of confidentiality must be reported to Jackie Mercer, Practice Manager and Data Protection Officer, or to Gill Suter, Assistant Practice Manager. All breaches will be recorded.

5.4 Abuse of privilege

The NHS Confidentiality Policy states the following:

- It is strictly forbidden for employees 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, staff must be aware of their personal responsibility and contractual obligations, and must undertake to abide by the policies and procedures of NHS England.

6 Disclosure

6.1 Disclosing information

The following list describes circumstances when information can be disclosed:[8]

- When effectively anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice[9]
- When the information is required by law or under a court order. In this situation, staff must discuss the matter with their line manager or Information Governance staff before disclosing, who will inform and obtain the approval of the practice Caldicott Guardian, Dr David Stainthorp

[8] NHS(E) Confidentiality Policy

[9] https://ico.org.uk/media/1061/anonymisation-code.pdf

- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of Patient Information) Regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority[10]. This is referred to as approval under s251 of the NHS Act 2006
- In Child Protection proceedings if it is considered that the information required is in the public's or child's interest. In this situation, staff must discuss the matter with their line manager or Information Governance staff before disclosing, who will inform and obtain the approval of the Caldicott Guardian (Dr Stainthorp)
- When disclosure can be justified for another purpose; this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation, staff must discuss the matter with their line manager or Information Governance staff before disclosing, who will inform and obtain the approval of the Caldicott Guardian
- The patient has the capacity to consent and consents to the disclosure
- It is required by statute, such as in relation to certain communicable diseases.

7 Audit

7.1 Good practice

With the advances of technology in healthcare, it is imperative that access is monitored and controlled in an effectual manner. Therefore, regular audits must be undertaken; this process will ensure that access to confidential information is gained only by those who are required to access it in the course of their normal duties.

All staff at Didcot Health Centre have a responsibility to participate in such audits and to comply with the subsequent recommendations. An audit template can be found at Annex A.

8 Summary

Confidentiality is the basis of trust between the patient and Didcot Health Centre. All staff must ensure that they are aware of their individual responsibilities and their duty to maintain patient confidentiality at all times.

Continued/...

[10] https://www.hra.nhs.uk/about-us/

Annex A – Audit guidance

Introduction

The purpose of a confidentiality audit is to identify if:

- Any confidentiality issues exist and, if so, to detail what they are
- Systems are at risk through deliberate misuse
- Existing controls are adequate and provide the necessary safeguards

The audit will also review:

- Local controls and processes regarding the access to, and use of, electronic data
- Local controls and processes regarding the access to, and use of, manual records
- Staff knowledge and awareness of their responsibilities and extant legislation regarding confidentiality

Didcot Health Centre is to ensure that there are appropriate confidentiality procedures in place in order to monitor access to personal confidential data.

Frequency

Confidentiality audits are to be undertaken through spot checks and questionnaires on a six monthly basis, and reports produced and retained for assurance purposes.

Assurance required

The table overleaf explains the criteria, assurances and evidence required for confidentiality audits.

Report template

Annex B gives an example of a confidentiality report template.

Level	Criterion	Assurance required	Source of assurance or evidence
1	There are documented confidentiality audit procedures in place that include the assignment of responsibility for monitoring and auditing access to confidential personal information. The procedures have been approved by senior management or committee and have been made available throughout the organisation.	Auditors require assurance that: • There are documented confidentiality audit procedures in place which include the assignment of responsibility for monitoring and auditing access to confidential personal information • The procedures have been approved by senior management or committee and have been made available throughout the organisation.	• Policy on confidential patient information • Standard procedures for monitoring and auditing access to patient information • Management approval of procedures (e.g., meeting minutes or other papers recording approval) • Documented assignment of responsibilities to job roles • Corresponding job descriptions • Publication of procedures throughout the organisation.
2	All staff members with the potential to access confidential personal information have been made aware of the procedures. The procedures have been implemented and appropriate action is taken where confidentiality processes have been breached.	Auditors require assurance that: • The training provided for staff who are conducting audits and investigating alerts is comprehensive, clear and unambiguous about the action to be taken • The written procedures for confidentiality audit and monitoring are implemented in the organisation • Appropriate disciplinary and remedial actions are taken where confidentiality processes have been breached • All staff members with the potential to access confidential patient information are aware of the audit procedures; and • The audit procedures are widely accessible	As above, plus: • Training records for staff carrying out audits and investigations • Descriptions of training provided • Corporate security and human resources procedures • Incident log of confidentiality alerts • Reports of the subsequent disciplinary actions taken • Minutes detailing committee reviewing confidentiality issues and performance • Availability of organisation's confidentiality, security and employment procedures to relevant staff • Methods used to make relevant current staff aware of the confidentiality audit procedures and disciplinary sanctions. This might take many forms, such as awareness sessions, as part of mandatory training, team discussions or distributions to staff • For relevant new joiners, evidence of induction training on confidentiality requirements and audit

3	Access to confidential personal information is regularly reviewed. Where necessary, measures are put in place to reduce or eliminate frequently encountered confidentiality incidents or events.	Auditors require assurance that: • The procedures for confidentiality audits and monitoring are regularly reviewed for scope and depth • Identified vulnerabilities are recorded, solutions are identified and problems resolved; and • Staff effectiveness in relation to confidentiality audits and monitoring is maintained, e.g., by appropriate ongoing training	As above, plus: • Reports from reviewing the audit and monitoring process • Security incidents and events relating to confidentiality • Risk register including identified confidentiality vulnerabilities • Reports of procedural and/or security changes, resulting from alerts or identified risks • Updated procedures and policy from lessons learned

Annex B – Example of an audit report template

Didcot Health Centre	Date of audit:	Audit reference no: [01/19] Page [1] of [2]
Summary of audit:		
Name of auditor(s):		
Date audit carried out:		
Date audit closed:		

Didcot Health Centre	Date of audit:	Audit reference no: [01/17] Page [2] of [2]
Summary of observations:		
Observation reference:	Description of observation:	
Summary of agreed actions:		
Reference:	Action required:	By whom & date:
Agreed follow-up/review:		
Name & signature of auditor(s):	Date closed:	
Additional comments:		
Name & signature of auditor(s):	Final closure date:	