Protocol: Caldicott Policy
Agreed By: The Partners of Cloister Road Surgery
Reviewed: Annually
Latest review date: 09 July 2019 (SD & MN)

Cloister Road Surgery

CALDICOTT POLICY

Table of contents

Protocol: Caldicott Policy
Agreed By: The Partners of Cloister Road Surgery
Reviewed: Annually
Latest review date: 09 July 2019 (SD & MN)

1 Introduction

1.1 Policy statement

The purpose of this document is to ensure that all staff at Cloister Road Surgery fully understand the requirement to adhere to the Caldicott principles, which were designed to safeguard and govern the use of patient information in all health and social care organisations.

1.2 Status

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment.

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 and other individuals performing functions in relation to the practice, such as agency workers, locums and contractors.

2.2 Why and how it applies to them

All staff at Cloister Road Surgery are to be fully conversant with this policy and are to understand the requirement for effective controls of personal confidential data (formerly patient identifiable information). This policy supports the Caldicott Report written in 1997, which provides guidance for the NHS regarding the use of confidential data. Orginially formed of six principles, a review took place by Dame Fiona Caldicott and in 2013 a seventh principle was introduced.

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.

3 Guidance

3.1 Caldicott guardians

A Caldicott guardian is a senior person within a health or social care organisation who ensures that personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained.

The Caldicott guardian for Cloister Road Surgery is Dr Sudha Dhall.

3.2 Caldicott lead or Information Governance lead

Individual practices are not required to have their own Caldicott guardian. However, they are to have in place a Caldicott lead or information governance (IG) lead. This is usually a senior clinician, although a non-clinical person may be appointed as the IG/Caldicott lead. If this is the case, they are to be supported by an appropriate clinician.

The IG leadfor Cloister Road Surgery is Dr Sudha Dhall (GP Principal).

3.3 Caldicott principles

The seven Caldicott principles are[1]:

1. **Justify the purpose(s)**

   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data**

   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis**

[1] A Manual for Caldicott Guardians

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities**

   Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law**

   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality**

   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

3.4 Compliance

All staff are to comply with the seven Caldicott principles and should any doubt arise regarding compliance, they are to contact the Dr Sudha Dhall. The patients of Cloister Road Surgery entrust staff to uphold confidentiality at all times, doing so in confidence. It is essential that patients are informed of the circumstances in which their personal confidential data may be shared in order to deliver safe and effective care.

Patients at Cloister Road Surgery are to be informed of the intended use of their information and this practice will adhere to the NHS confidentiality model[2]:

PROTECT – look after the patient's information

INFORM – ensure that patients are aware of how their information is used

PROVIDE CHOICE – allow patients to decide whether their information can be disclosed or used in particular ways

IMPROVE – always look for better ways to protect, inform and provide choice

[2] Confidentiality NHS Code of Practice

Furthermore, Cloister Road Surgery will ensure the following preventative measures are adopted:

- All personnel are aware of their responsibilities regarding confidentiality; this includes visitors, contractors and volunteers
- The recording of patient information will be accurate and consistent
- Patient information will be kept confidential
- Patient information will be stored securely (be it electronically or hard copies)
- The disclosure of such information will be done with due diligence

Staff must ensure they report any breaches or risks to the Dr Sudha Dhall immediately.

3.5 Data Security and Protection Toolkit

The NHS Data Security and Protection Toolit (DSPT) is an online self-assessment tool which enables Cloister Road Surgery to assess their performance agains the National Data Guardian's 10 data security standards. This is a mandaroty requirement which will ensure compliance in line with the General Data Protection Regulation (GDPR).

Cloister Road Surgery will undertake an assessment to demonstrate that the practice can be trusted to maintain the confidentiality and security of personal information, thus reducing the number of individuals who 'opt out' of the sharing of their personal identifiable data.[3]

To demonstrate compliance, Cloister Road Surgery will submit an assessment no later than 31st March each year.

Cloister Road Surgery will use the DSPT assertations action plan for GPs and the DSPT staff awareness questions to ensure the pracitce achieves a successful outcome for the assessment.

Further information regarding the DSPT is available in the pracitce DSPT policy.

3.6 Audit

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 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 Cloister Road Surgery have a responsibility to participate in such audits and to comply with the subsequent recommendations.

Audit guidance and relevant templates can be found at Annex A.

3.7 Summary

[3] NHS About the Data Security and Protection Toolkit

Protocol: Caldicott Policy
Agreed By: The Partners of Cloister Road Surgery
Reviewed: Annually
Latest review date: 09 July 2019 (SD & MN)

At Cloister Road Surgery all staff are aware of the Caldicott principles and that they have a duty to ensure they remain compliant at all times. Compliance will be monitored through annual audit and all staff will be briefed regarding the findings and subsequent recommendations.

Any questions relating to this policy or the practice of retaining good electronic records should be directed to the undersigned in the first instance.

Magdalena Nagadowska
Practice Manager
Cloister Road Surgery

July 2019

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

Cloister Road Surgery 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 6 monthly basis and reports produced and retained for assurance purposes.

Assurance required

The table overleaf explains the criterion, assurance and evidence required for confidentiality audits as detailed in the IG toolkit.

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 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.	• Policy on confidential patient information. • Standard procedures for monitoring and auditing access to patient information. • Management approval of procedures (for example, 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 conducting audits and investigating alerts is comprehensive, clear and unambiguous on 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	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 of 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

		accessible.	procedures and disciplinary sanctions. This might have 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 on confidentiality audits and monitoring is maintained, for example, by appropriate ongoing training.	As above plus: • Reports from reviewing the audit and monitoring process. • Security incidents and events related 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.

Table 1.0 – Assurance required – Source – www.igt.hscic.gov.uk

Annex B – Example of an audit report template

Cloister Road Surgery	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:		

Cloister Road Surgery	Date of audit:	Audit reference no: [01/19]

		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:	