Caldicott and Confidentiality Policy

Version	Edited by	Date issued	Next review date

Key personnel identified within this policy

Position	Named individual
Data Controller	Fiona Butcher
Caldicott Guardian	Dr Zammad Chishti /Fiona Butcher
Practice Manager	Fiona Butcher

Table of contents

1 Introduction

1.1 Policy statement

This policy explains and enforces the obligations of Caldicott, confidentiality and non-disclosure among the employees of this organisation. This applies to information generated, held and processed by the organisation. Furthermore, it outlines the principles that are to be adhered to by all staff at this organisation to understand the requirement for effective controls of personal confidential data (formerly patient identifiable information).

For further detailed information, see the organisation's Confidentiality and Data Protection Handbook.

1.2 Status

In accordance with the Equality Act 2010, we have considered how provisions within this policy might impact on different groups and individuals. This document and any procedures contained within it are non-contractual, which means they may be modified or withdrawn at any time. They apply to all employees and contractors working for the organisation.

2 Caldicott

2.1 Caldicott principles

The Caldicott Principles are as detailed within the NDG document titled The Eight Caldicott Principles.

2.2 Caldicott Guardian role

The Manual for Caldicott Guardians details the role of the Caldicott Guardian while the NDG document Guidance about the appointment of Caldicott Guardians, their role and responsibilities provides additional information. Caldicott Guardians may also seek guidance from the UK Caldicott Guardian Council (UKCGC).

2.3 Caldicott Guardian and/or Information Governance Lead

This organisation is required to have its own Caldicott Guardian and this is normally a senior clinician. This role is also given an additional title of Information Governance (IG) Lead. Should a non-clinical person be appointed as the Caldicott Guardian, they should be supported by an appropriate clinician.

All staff are to be aware of who the Caldicott Guardian/IG lead is. This information should be added to the Responsible Persons list and made freely available. Furthermore, the details of this organisation's Caldicott Guardian are to be recorded on the Caldicott Guardian Register and must be kept up to date at all times.

3 Confidentiality

3.1 Requirement

The NHS Confidentiality Policy and the NHS Confidentiality Code of Practice state that all staff working in the NHS are bound by a legal duty of confidence to protect personal information they may encounter during their work. This is not purely a requirement of their contractual responsibilities; it is also a requirement within the common law duty of confidence.

3.2 NHS Confidentiality Code of Practice

All staff are to adhere to the principles of confidentiality outlined in the NHS Confidentiality Code of Practice:

- 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 a line manager
- Patients are to be informed of the intended use of their information and this organisation will adhere to the detailed requirements shown at Annex A to the code

This organisation will ensure that the requirements within the above Code of Practice are strictly followed, and that staff will immediately report any breaches of confidence or potential risks to the Caldicott Guardian or IG Lead.

3.3 Non-disclosure of information

All employees must adhere to the clauses outlined in their individual contract of employment in relation to confidentiality, data protection and intellectual property.

3.4 Breach of confidential information

Any breach of confidentiality will be managed in accordance with the organisation's Information Governance Breach Reporting Policy.

3.5 Third-party requests for information

Any employee approached by a third party, including any media source, and asked to make comments or provide information relating to the organisation and its affairs (or the affairs of its patients, partners, employees, contractors or any business associate) must not, under any circumstances, respond without having sought permission and guidance from the Practice Manager. The Practice Manager will then discuss the request with the partners and consider asking for assistance from the press information/media officer at the ICB.

3.6 Whistleblowing or protected disclosures

In respect of any malpractice or unlawful conduct, any employee is entitled to submit a protected disclosure under the organisation's Freedom to Speak Up Policy and Procedure (or Whistleblowing Policy). Further detailed information can be found in NHS England's Freedom to Speak Up guidance document.

3.7 Disclosing information

The GMC offers guidance in the document titled Disclosing patients' personal information: a framework. Supporting information can also be found in the organisation's Consent Guidance.

3.8 Protecting information under the Gender Recognition Act

Section 22 of the Gender Recognition Act 2004 states that it is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.

This is classified as *protected information* and is defined in Section 22(2) as information relating to a person who has applied for a Gender Recognition Certificate (GRC) under the Act, and which concerns that application (or a subsequent application by them) or their gender prior to being granted a full GRC.

While Section 22 is a privacy measure that prevents officials from disclosing that a person has a trans history, there are exemptions for medical professionals as detailed within Statutory Instrument 2005 No.635 (Section 5) provided all the following circumstances apply:

- The disclosure is made to a health professional
- The disclosure is made for medical purposes; and
- The person making the disclosure reasonably believes that the subject has given consent to the disclosure or cannot give such consent

As a precautionary measure, it is good practice to apply the Section 5 criteria to all disclosures of information about the trans status of a patient. Furthermore, patients should never be asked to produce a GRC to 'prove' their trans status.

3.9 Confidentiality and non-disclosure agreement

All persons engaged to work for and on behalf of the organisation will be required to sign the confidentiality and non-disclosure agreement to be found at Annex A. A signed copy will be held on the individual's personnel file. Visitors to the organisation will also be expected to

sign the organisation's third-party confidentiality agreement incorporating fire safety and risk awareness for visitors.

3.10 National data opt-out

The national data opt-out or (NDO-O) is a service that allows patients to opt out of their confidential patient information being used for research and planning. Additional information can be found in the National data opt-out guidance.

3.11 Abuse of privilege

As detailed in the NHS Confidentiality Policy, 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 2018, and disciplinary action may be taken.

3.12 Privacy notices

The Practice Privacy Notice explains to patients the ways in which the organisation gathers, uses, discloses and manages a patient's data. It fulfils a legal requirement to protect a patient's privacy. Other privacy notices are provided for the following:

- Children
- Employee
- Candidates applying for work

4 Compliance

4.1 Good practice

To support the NHS Code of Practice, the following actions will be undertaken:

- Person-identifiable information will be anonymised so far as is reasonably practicable, while being mindful of not compromising the data
- Access to consulting rooms, administrative areas and record storage areas will be restricted
- All staff should always maintain a clear desk routine. No patient confidential information is to be left unattended in any unsecured area, at any time
- All IT equipment is to be shut down at the end of the working day except any that is required to remain left on such as server equipment
- Smartcards are to be removed from the computer whenever the user leaves their workstation, as per the Smartcard Policy
- Confidential waste is shredded or disposed of appropriately and as per the Confidential Waste Policy

- Staff will not talk about patients or discuss confidential information in areas where they may be overheard

The organisation's Communication Policy provides advice on disclosing information electronically or via telephone to a patient, proxy or third party.

4.2 Audit

Regular audits must be undertaken to ensure access to confidential information is gained only by those who are required to access it in the course of their normal duties. Audit guidance and templates can be found at Annex B and Annex C.

4.3 Additional compliance tools

In addition to audit, there are further tools that can be used to support such as:

- All members of the organisation will undergo annual confidentiality training
- A confidentiality quiz detailing different scenarios is available at Annex D