**ISSA MEDICAL GROUP**

**Main Site: Issa @ Deepdale**

**Branch Site: Issa @ Fulwood**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date of Review (Version):** | **Next Review Date:** | **Edited by:** | **Approved by:** | **Comments:** |
| **14.6.23** | **13.6.24** | **D Robinson** |  | **Old Policy deleted and one from FPM updated and adapted** |
| **6.7.23** | **6.7.24** | **S Nixon** |  | **Changes approved by B. Vernon – removal of non-clinical guardian** |
| **29.4.24** | **29.4.25** | **S. Nixon** |  | **Updated from Practice Index** |
|  |  |  |  |  |

**CALDICOTT AND CONFIDENTIALITY POLICY**

**CALDICOTT GUARDIAN Dr Z Patel**

# Introduction

## Policy statement

This policy explains and enforces the obligations of Caldicott, confidentiality and non-disclosure among the employees of Issa Medical. 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).

The Caldicott principles are derived from the Dame Fiona Caldicott [Information Governance Review in 2013](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf) which now forms the [Caldicott Guardian guidance](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013756/Caldicott_Guardian_guidance_v1.0_27.08.21.pdf) from the National Data Guardian (NDG). All staff are to fully understand the requirement to adhere to the Caldicott principles which are designed to safeguard and govern the use of patient information in all health and social care organisations.

The [NHS Confidentiality Policy](https://www.england.nhs.uk/wp-content/uploads/2019/10/confidentiality-policy-v5.1.pdf) and the [NHS Confidentiality Code of Practice](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf) 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.

Staff are to be reminded that information classed as [objective knowledge](https://classroom.synonym.com/examples-objective-knowledge-23431.html) relates to the affairs of the organisation. This may include information regarding:

|  |  |
| --- | --- |
| * Partners | * Contractual arrangements |
| * Employees | * Dealings |
| * Patients | * Transactions |
| * Contractors | * Policies and procedures |
| * Business associates | * Decisions |
| * Suppliers | * Technology and systems |
| * Market information | * Any other organisational confidential matter |

The reputation and continuing ability of the organisation to work effectively in the position of trust and responsibility it holds (which is also reflected in the trust and responsibility held by those persons engaged by the organisation to work on its behalf) rely on confidential information being held as confidential.

Legislation and national guidance documents relating to both confidentiality and Caldicott can be found at Annex A.

## Status

The organisation 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](https://www.legislation.gov.uk/ukpga/2010/15/contents). Consideration has been given to the impact this policy might have with regard to the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the practice such as agency workers, locums and contractors.

# 2 Caldicott

## 2.1 Caldicott principles

The Caldicott Principles are as detailed within the NDG document titled [The Eight Caldicott Principles](https://www.gov.uk/government/publications/the-caldicott-principles).

## 2.2 Caldicott Guardian role

A Caldicott Guardian’s role, as outlined within the [Manual for Caldicott Guardians](https://www.ukcgc.uk/caldicott-guardians-manual), 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’s main concern is information relating to individuals and their care. Additionally, this need for confidentiality also extends to other individuals and this includes relatives, staff and others.

Further information with regard to the role of the Caldicott Guardian and who organisations need to appoint and the expected competencies can be sought in the NDG document [Guidance about the appointment of Caldicott Guardians, their role and responsibilities](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013756/Caldicott_Guardian_guidance_v1.0_27.08.21.pdf).

## 2.3 Caldicott Guardian and/or Information Governance Lead

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

Further guidance on Caldicott Guardianship can be found at this [Gov.uk](https://www.gov.uk/government/groups/uk-caldicott-guardian-council) site, although the Manual for Caldicott Guardians should be the starting point for those who are newly appointed or as a reference point for existing Caldicott Guardians.

All staff are to be aware of who the Caldicott Guardian/Information Governance lead is.

## 2.4 Caldicott Guardian registration

The UKCGC states that all organisations that are required to have a Caldicott Guardian should ensure their up-to-date details are on the [Caldicott Guardian Register](https://digital.nhs.uk/services/organisation-data-service/update-your-data/registers).

The register is used by NHS E to store and update Caldicott Guardians’ details and by the UK Caldicott Guardian Council to facilitate contact and the dissemination of information.

## 2.5 UK Caldicott Guardian Council (UKCGC)

The [UK Caldicott Guardian Council](https://www.ukcgc.uk/) (UKCGC) is the national body for Caldicott Guardians within the UK. The UKCGC provides support for Caldicott Guardians and others fulfilling the Caldicott function within the organisation.

The UKCGC helps to uphold the eight Caldicott principles.

# Confidentiality

## 3.1 Requirement

All employees must, from the date of the commencement of employment or other form of engagement, and thereafter, observe strict confidentiality in respect of any information held by the organisation and by each individual working on behalf of the organisation. This includes dealings, transactions, procedures, policies, decisions, systems and other matters of a confidential nature concerning the organisation and its affairs.

Other than in the proper course of their duties, employees must not, either during or at any time after the termination of their employment, exploit or disclose confidential information. In addition, employees must not, through negligence, wilful misconduct, or inadvertence, allow the use, exploitation or disclosure of any confidential information relating to the affairs of the organisation, its patients, partners, employees, contractors, business partners or suppliers.

## NHS Confidential Code of Practice

All staff are to adhere to the principles of confidentiality outlined in the [NHS Confidentiality Code of Practice](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf):

* 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/ IG Lead.

## Non-disclosure of information

All employees must, from the beginning of their employment with the organisation and after the termination of their employment with the organisation, observe strict confidentiality and non-disclosure in respect of any information held by the organisation, except when required or authorised to disclose such information by the organisation or by law.

It is an obligation upon all employees during employment, or engaged under other contractual arrangements, to maintain information in confidence and not, directly or indirectly, disclose it other than for the purposes it was gathered. Any such information in the possession of an individual, either in electronic format or hard copy, shall be returned to the organisation before or at the point in time that employment ceases, however such cessation occurs.

Following the cessation of employment, or other contractual engagement with the organisation, an individual must not, directly or indirectly, use for gain, discuss or pass on to others confidential information that can be classed as objective knowledge in that it has been gained during the course of their employment.

This includes information relating to that as previously listed at Section 1.1.

NOTES:

* While information must not be improperly disclosed and must be used only for the purpose for which it was gathered, nothing prevents an employee or other individual making a protected disclosure under the [Public Interest Disclosure Act 1998](http://www.legislation.gov.uk/ukpga/1998/23/contents) in respect of any malpractice or unlawful conduct.
* At this organisation, personal information relating to staff is managed and stored and the same standards are applied to their information as are applied to the confidentiality of patient information.

## Breach of Confidential Information

Any breach of confidentiality, particularly involving data, could have major negative consequences for this organisation and the individual. The organisation will therefore take the appropriate disciplinary action against any employee who commits a breach of confidentiality by reporting it to the organisation’s Data Protection Officer Dawn Robinson (DPO).

If it is a serious breach, the DPO will be bound to recommend that it is [reported](https://ico.org.uk/for-organisations/report-a-breach/) to the Information Commissioner’s Office (ICO) who may, in turn, institute criminal proceedings against the individual and, if found to be negligent, the organisation itself. The individual, if found guilty, will be required to pay a fine and acquire a criminal record and the organisation may be heavily fined if found guilty.

There must be no attempt to use any confidential information in a manner that may either directly or indirectly cause, or be calculated to cause, injury or loss to the organisation.

Further reading can be sought from the Information Governance Breach Reporting Policy.

## 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 Mrs S Riley Senior Practice Manager.

The manager will then discuss the request with the partners and consider asking for assistance from the press information/media officer at the ICB.

## 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. This states that protected disclosures can be made to a Partner, Practice Manager or the nominated Freedom to Speak up Guardian (FSUG).

Legislation in the UK was enacted by the Public Interest Disclosure Act 1998 to enable employees and other persons such as agency temporary workers to disclose genuine concerns, especially those that seem to involve unlawful conduct or malpractice. This also protects them from any form of victimisation arising from making such a disclosure.

Further guidance can be sought from the NHS E document [Freedom to Speak Up](https://www.england.nhs.uk/ourwork/freedom-to-speak-up/).

## Disclosing Information

The GMC offers guidance in the document titled [Disclosing patients’ personal information: a framework](https://www.gmc-uk.org/professional-standards/professional-standards-for-doctors/confidentiality/disclosing-patients-personal-information-a-framework).

**3.8 Protected information under the Gender Recognition Act**

[Section 22](https://www.legislation.gov.uk/ukpga/2004/7/section/22) of the [Gender Recognition Act 2004](https://www.legislation.gov.uk/ukpga/2004/7/contents) 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](https://www.gov.uk/apply-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)](https://www.legislation.gov.uk/uksi/2005/635/article/5/made) provided all of 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

## 3.9 Trans Status

Patients should never be asked to produce a GRC to ‘prove’ their trans status. The GRC is not a requirement, and many trans people simply choose not to have one while others may not yet meet the eligibility criteria.

As a precautionary measure, it is good practice to apply the Section 5 criteria set out in Section 3.8 to all disclosures of information about the trans status of a patient. The reason being is that it may not be accurately known whether the person has a GRC or not. Additionally, the general protocols on medical confidentiality and information governance apply to all patients whether they have a GRC or not.

NOTE:  
  
Pride in Practice has advised that good information governance around this subject is essential because unlawful and unwarranted disclosures of a person’s trans status leave organisations open to legal proceedings and, in doing so, can have serious and unforeseen consequences in ‘outing’ trans people.

## 3.10 Confidentiality and non-disclosure agreement

All persons engaged to work for and on behalf of the organisation will be required to sign the confidentiality agreement which is found on Clarity. A signed copy will be held on the individual’s personnel file.

Visitors to the organisation will also be expected to sign a third party confidentiality agreement which can be found on Clarity.

## 3.11 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. NDO-O was introduced in England along with the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) and GDPR on 25 May 2018. This followed recommendations from the NDG that patients should be able to opt-out of their personal confidential data being used for purposes other than their direct medical care.

Further reading to support the [Data Security and Protection Toolkit (DSPT)](https://www.dsptoolkit.nhs.uk/) can be sought from NHS E [National data opt-out](https://digital.nhs.uk/services/national-data-opt-out) guidance.

## 3.12 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 2018.

* 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.

## 3.13 Confidentiality awareness and informing

To ensure that any user of our services, our staff and potential employees are aware of the confidentiality obligations within this organisation, privacy notices are available.

There is a staff privacy note in the recruitment policy on Clarity.

The privacy notice for patients 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 and can also be found on Clarity.

# Compliance

## Good practice

To support the [NHS Code of Practice](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf), the following actions will be undertaken to ensure that confidentiality is maintained:

* 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 such as server equipment or any that are being updated
* Smartcards are to be removed from the computer whenever the user leaves their workstation. The Smartcard Policy details the need for, and terms and conditions of, use of the NHS Smartcard
* 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

## Data Security and Protection Toolkit (DSPT)

There is a requirement to undertake an annual DSPT assessment to demonstrate that the organisation can be trusted to maintain the confidentiality and security of personal information.

To demonstrate compliance, this organisation is required to submit the assessment by 30 June annually. Further information can be found on the NHS E [Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/) webpage and the DSPT staff [awareness questions](https://www.dsptoolkit.nhs.uk/Help/staff-awareness-questions) for the current year’s standards to ensure the practice achieves a successful outcome for the assessment.

## Audit

Regular audits must be undertaken to ensure compliance. 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.

At this organisation, all staff have a responsibility to participate in such audits and to comply with the subsequent recommendations.

## Additional Compliance Tools

In addition to audit, all members of the organisation will undergo annual confidentiality training.

# Annex A – Legislation and guidance

The following legislation and guidance documents support both Caldicott and confidentiality:

* [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) (UK GDPR is detailed at Part 2)
* [EU General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN)\*
* [Freedom of Information Act 2000](https://www.legislation.gov.uk/ukpga/2000/36/contents)
* [Gender Recognition Act 2004](https://www.legislation.gov.uk/ukpga/2004/7/contents)
* [Health and Social Care (National Data Guardian) Act 2018](https://www.legislation.gov.uk/ukpga/2018/31/contents/enacted)
* [Human Rights Act 1998](https://www.legislation.gov.uk/ukpga/1998/42/contents/enacted)
* [National Health Service Act 2006](https://www.legislation.gov.uk/ukpga/2006/41/contents)
* [Public Interest Disclosure Act 1998](http://www.legislation.gov.uk/ukpga/1998/23/contents)
* [Caldicott review: Information: to share or not to share? The Information Governance Review](https://www.gov.uk/government/publications/the-information-governance-review) (April 2013)
* [The Caldicott Principles](https://www.gov.uk/government/publications/the-caldicott-principles) (December 2020)
* [Caldicott Principles: A consultation about revising, expanding and upholding the principles](https://www.gov.uk/government/consultations/caldicott-principles-a-consultation-about-revising-expanding-and-upholding-the-principles) (2020)
* [The Caldicott Committee Report on the Review of Patient-Identifiable Information (1997)](https://webarchive.nationalarchives.gov.uk/20130124064947/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf)
* [National Data Opt-out](https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out) (2022)
* NHS E [Records Management Code of Practice](https://transform.england.nhs.uk/information-governance/guidance/records-management-code/) (2023)
* NHS Digital [Code of practice on confidential information](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/code-of-practice-on-confidential-information) (2022)
* NHS Digital [A guide to confidentiality in Health and Social Care](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care) (2022)

\* EU GDPR as incorporated in English law by the EU (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (the “UK GDPR”)