**Caldicott and Confidentiality Policy**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| 1.0 | August 2025 | Amy Baker | Amy Baker | No change |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Contents**

[1 Introduction 3](#_Toc92184001)

[1.1 Policy statement 3](#_Toc92184002)

[1.2 Status 3](#_Toc92184003)

[1.3 KLOE (England only) 3](#_Toc92184004)

[1.4 Training and support 4](#_Toc92184005)

[2 Scope 5](#_Toc92184006)

[2.1 Who it applies to 5](#_Toc92184007)

[2.2 Why and how it applies to them 5](#_Toc92184008)

[2.3 Legislation and guidance 6](#_Toc92184009)

[2.4 UK General Data Protection Regulation 6](#_Toc92184010)

[2.5 National data opt-out (England only) 7](#_Toc92184011)

[3 Definition of terms 7](#_Toc92184012)

[3.1 Data Protection Act and UK GDPR 7](#_Toc92184013)

[3.2 Confidentiality 7](#_Toc92184014)

[3.3 Confidential information 7](#_Toc92184015)

[3.4 Protected disclosure 7](#_Toc92184016)

[3.5 Personal confidential data 8](#_Toc92184017)

[3.6 Caldicott principles 8](#_Toc92184018)

[3.7 Caldicott Guardian 8](#_Toc92184019)

[3.8 UK Caldicott Guardian Council (UKCGC) 8](#_Toc92184020)

[3.9 British Medical Association 8](#_Toc92184021)

[3.10 Care Quality Commission 8](#_Toc92184022)

[3.11 Data security and protection toolkit (DSPT) 9](#_Toc92184023)

[4 Guidance 9](#_Toc92184024)

[4.1 Confidentiality 9](#_Toc92184025)

[4.2 Non-disclosure of information 9](#_Toc92184026)

[4.3 Third-party requests for information 10](#_Toc92184027)

[4.4 Whistleblowing or protected disclosures 10](#_Toc92184028)

[4.5 Confidentiality and non-disclosure agreement 10](#_Toc92184029)

[4.6 Caldicott Guardian role 11](#_Toc92184030)

[4.7 Caldicott Guardian and/or Information Governance Lead 11](#_Toc92184031)

[4.8 Caldicott Guardian registration 11](#_Toc92184032)

[4.9 Caldicott principles 12](#_Toc92184033)

[5 Compliance 13](#_Toc92184034)

[5.1 General 13](#_Toc92184035)

[5.2 NHS Confidential Code of Practice 13](#_Toc92184036)

[5.3 Practice privacy notices 15](#_Toc92184037)

[5.4 Data Security and Protection Toolkit (DSPT) 15](#_Toc92184038)

[5.5 Audit 16](#_Toc92184039)

[5.6 Additional compliance tools 16](#_Toc92184040)

[6 Confidentiality in practice 16](#_Toc92184041)

[6.1 Good practice 16](#_Toc92184042)

[6.2 Confidentiality breach 17](#_Toc92184043)

[6.3 Abuse of privilege 17](#_Toc92184044)

[7 Disclosure 17](#_Toc92184045)

[7.1 Disclosing information 17](#_Toc92184046)

[8 Summary 18](#_Toc92184047)

**Annexes are on a separate document -**

**Caldicott and Confidentiality Policy Annexes A-D**

[Annex A – Confidentiality and non-disclosure agreement](#_Toc92184048)

[Annex B – Audit guidance](#_Toc92184049)

[Annex C – Example of an audit report template](#_Toc92184050)

[Annex D – Confidentiality quiz](#_Toc92184051)

# Introduction

## Policy statement

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 and the NHS Care Record Guarantee. The latter is produced to assure patients regarding the use of their information.[[1]](#footnote-1)

This policy also explains and enforces the obligations of confidentiality and non-disclosure among the employees of our organisation. This applies to information generated, held and processed by the organisation.

This policy is to be read in conjunction with the Contract of Employment and the organisation’s privacy notices and in conjunction with an individual’s contract of employment where this contains a confidentiality agreement.

Further information on privacy notices can be seen at [Section 5.3](#_Practice_privacy_notices).

Lastly, 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.

## 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. For the avoidance of doubt, it does not form part of your contract of employment.

## Training and support

The organisation will provide guidance and support to help those to whom it applies to 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.

[](https://practiceindex.co.uk/gp/forum/threads/whistleblowing.13865/)

Caldicott and confidentiality training is available on the [HUB](https://hub.practiceindex.co.uk/courses#collapse_1293).

# Scope

## Who it applies to

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.

Furthermore, it applies to clinicians who may or may not be employed by the organisation but who are working under the Additional Roles Reimbursement Scheme (ARRS)[[2]](#footnote-2).

## Why and how it applies to them

This policy outlines the principles that are to be adhered to by all staff at our organisation to understand the requirement for effective controls of personal confidential data (formerly patient identifiable information).

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, employees, patients, contractors, business associates, suppliers, market information, contractual arrangements, dealings, transactions, policies, procedures, decisions, technology and systems.

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.

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. It must not be improperly disclosed and must be used only for the purpose for which such information was gathered.

Any breach of confidentiality, particularly involving data, could have major negative consequences for our 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 (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.

Nothing in this policy 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.

The Caldicott principles are derived from the Dame Fiona Caldicott Information Governance Review in 2013[[3]](#footnote-3) which now forms the current Caldicott Guardian guidance that was published in September 2021 from the National Data Guardian (NDG)[[4]](#footnote-4).

## Legislation and guidance

In addition to the NDG guidance relating to the current Caldicott Guardian guidance, throughout this policy and any supporting references, the following legislation and guidance documents are referred to:

* [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)
* [Human Rights Act 1998](https://www.legislation.gov.uk/ukpga/1998/42/contents/enacted)
* [Freedom of Information Act 2000](https://www.legislation.gov.uk/ukpga/2000/36/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)
* [The Health and Social Care (National Data Guardian) Act 2018](https://www.legislation.gov.uk/ukpga/2018/31/contents/enacted)
* [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted)
* [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 Principles](https://www.gov.uk/government/publications/the-caldicott-principles) (December 2020)
* [National Health Service Act 2006](https://www.legislation.gov.uk/ukpga/2006/41/contents)
* [EU General Data Protection Regulation](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN) 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”)
* [National Data Opt-out](https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out) (2021)
* [Records Management Code of Practice](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/) (2021)

## UK General Data Protection Regulation

The Data Protection Act 2018 (DPA 2018) sets out the framework for data protection law in the UK. It sits alongside and supplements the UK General Data Protection Regulation (UK GDPR).[[5]](#footnote-5)

## National data opt-out (England only)

National Data Opt-Out (NDO-O) was introduced along with the Data Protection Act 2018 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.

The NDG states that *“A patient should be able to state their preference once (online or in person), confident in the knowledge that this will be applied across the health and social care system”.*

Further reading can be sought from the [National data opt out guidance](https://practiceindex.co.uk/gp/forum/resources/national-data-opt-out-guidance.1395/) document.

NDO-O only applies to all general practices in England.

# Definition of terms

## Data Protection Act and UK GDPR

The UK GDPR came into effect as of 1 January 2021, replacing the EU GDPR which had been in place since 25 May 2018. The UK GDPR is incorporated as Part 2 within the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) (DPA18).

Further reading can be found in the [UK GDPR policy](https://practiceindex.co.uk/gp/forum/resources/uk-gdpr-policy.1703/).

## Confidentiality

The principle of keeping secure and secret from others, information given by or about an individual during a professional relationship[[6]](#footnote-6)

## Confidential information

“Confidential information” means any information processed by the organisation or supplied (whether supplied in writing, orally or otherwise) by the organisation or gathered by an individual in relation to the performance of his/her duties that is marked as “confidential”.

Confidential information in relation to patients is defined in NHS Digital’s operational guidance document[[7]](#footnote-7) and is also defined within the [National Health Service Act 2006](https://www.legislation.gov.uk/ukpga/2006/41/contents).

## Protected disclosure

The protected disclosure of unlawful conduct, malpractice or wrongdoings within the organisation is commonly known as “[whistleblowing](https://www.england.nhs.uk/ourwork/whistleblowing/)”.

## Personal confidential data

This is information that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number, etc.[[8]](#footnote-8)

## Caldicott principles

Caldicott principles apply to the use of confidential information within health and

social care organisations and when such information is shared with other

organisations and between individuals, both for individual care and for other

purposes.

Further information on the Caldicott principles can be found at [Section 4.4](#_Caldicott_principles).

## Caldicott Guardian

The Caldicott Guardian is to provide leadership and informed guidance on complex matters involving confidentiality and information sharing. This role is key in ensuring that our organisation satisfies the highest practical standards for handling personal confidential data information.

## UK Caldicott Guardian Council (UKCGC)

The UKCGC is the national body for Caldicott Guardians within the UK. The [UK Caldicott Guardian Council](https://www.ukcgc.uk/) provides support for Caldicott Guardians and others fulfilling the Caldicott function within the organisation. This includes specific support for Caldicott Guardians during the COVID-19 pandemic.

The UKCGC helps to uphold the eight Caldicott principles.

## British Medical Association

The [British Medical Association](https://www.bma.org.uk/about-us) (BMA) is the trade union and professional body for doctors in the United Kingdom.

## 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 encourages services to improve.[[9]](#footnote-9)

## Data security and protection toolkit (DSPT)

The [NHS Data Security and Protection Toolkit](https://www.dsptoolkit.nhs.uk/News/2021-2022-standard) version 4 (2021/22) is an online self-assessment tool that enables our organisation to assess its performance against the 10 data security standards of the National Data Guardian.

This is a mandatory requirement which will ensure compliance in line with UK GDPR.

# Guidance

## Confidentiality

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.

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.

## Non-disclosure of information

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:

* Partners
* Employees
* Contractors
* Patients
* Business associates
* Suppliers
* Market information
* Contractual arrangements
* Dealings
* Transactions
* Policies and procedures
* Decisions
* Technology and systems
* Any other matters relating to a confidential nature concerning the organisation

## 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 organisation’s information governance team.

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

## 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 Whistleblowing Policy.

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. The legislation also protects them from any form of victimisation arising from making such a disclosure.

The organisation’s Whistleblowing Policy provides a procedure for making protected disclosures. This states that protected disclosures are normally made to the Strategic Business Manager or a Partner. If the individual employee feels unable to report the matter internally then they are free to report it to an external organisation.

This organisation’s external whistleblowing contact is the Local Medical Committee (LMC) to whom concerns may be expressed.

Refer to the [Whistleblowing Policy and Procedure](https://practiceindex.co.uk/gp/forum/resources/whistleblowing-policy-and-procedure.469/)

## 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](#_Annex_A_-).

A signed copy will be held on the individual’s personnel file.

Visitors to the organisation will also be expected to sign a confidentiality agreement and this document also incorporates fire safety and risk awareness for visitors. Further information can be found at:

[Third-party confidentiality agreement incorporating fire safety and risk awareness for visitors](https://practiceindex.co.uk/gp/forum/resources/third-party-confidentiality-agreement-incorporating-fire-safety-and-risk-awareness-for-visitors.1391/)

## Caldicott Guardian role

A Caldicott Guardian’s role, as outlined within the Manual for Caldicott Guardians, 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.

At our organisation, we store, manage and share personal information relating to staff and the same standards are applied to their information as are applied to the confidentiality of patient information.

Further information with regard to the role of the Caldicott Guardian and who organisations need to appoint and their expected competencies can be sought in the National Data Guardian document titled [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).

## Caldicott Guardian and/or Information Governance Lead

Practices are required to have their own Caldicott Guardian.

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.

The Caldicott Guardian for our organisation is Jennifer Wain, our Strategic Business Manager. They are supported by our GP Lead for Clinical Governance.

## 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 Digital to store and update Caldicott Guardians’ details and by the Council to facilitate contact and dissemination of information.

## Caldicott principles

In September 2020, it was agreed that the wording of the existing principles should be altered and a further principle would be added. This is detailed within the National Data Guardian document titled [The Eight Caldicott Principles](https://www.gov.uk/government/publications/the-caldicott-principles) dated December 2020.

**Principle 1:**

Justify the purpose(s) for using confidential information. Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented with continuing use regularly reviewed by an appropriate guardian.

**Principle 2:**

Use confidential information only when it is necessary. Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

**Principle 3:**

Use the minimum necessary confidential information. Where the use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

**Principle 4:**

Access to confidential information should be on a strict need-to-know basis. Only those who need access to confidential information should have access to it and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

**Principle 5:**

Everyone with access to confidential information should be aware of their responsibilities. Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.  
  
**Principle 6:**

Comply with the law. Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with the legal requirements set out in statute and under common law.  
  
**Principle 7:**

The duty to share information for individual care is as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles.

They should be supported by the policies of their employers, regulators and professional bodies.

**Principle 8:**

Inform patients and service users about how their confidential information is used. A range of steps should be taken to ensure no surprises for patients and service users so they can have clear expectations about how and why their confidential information is used and what choices they have about this. These steps will vary depending on the use.

As a minimum, this should include providing accessible, relevant and appropriate information – in some cases, greater engagement will be required.

# Compliance

## General

All staff are to comply with the confidentiality requirements as detailed within the eight Caldicott principles.

Should any doubt arise regarding compliance, they are to contact the Caldicott Guardian. The patients of our organisation entrust staff to always uphold confidentiality, doing so with confidence. It is essential that patients are informed of the circumstances in which their personal confidential data may be shared to deliver safe and effective care.

## NHS Confidential Code of Practice

All staff at our organisation 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) dated November 2003:

* 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
* Patients at our organisation 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.

The main headings within the Code of Practice are:

**Protect patient information (A1)**

Protect the patient’s information through a number of measures:

* Recognising that confidentiality is an obligation for all staff, external contractors and volunteers
* Recording patient information accurately and consistently
* Keeping patient information private
* Keeping patient information physically and electronically secure

**Inform patients effectively – no surprises (A2)**

Ensure that patients are aware of how their information is used:

* Check that patients have seen the available information leaflets
* Make clear to patients when information is recorded or health records are accessed
* Make clear to patients when information is or may be disclosed to others
* Check that patients are aware of the choices available in respect of how their information may be used or shared
* Check that patients have no concerns or queries about how their information is used
* Answer any queries personally or direct patients to others who can answer their questions or to other sources of information
* Respect the right of patients to have access to their health records
* Communicate effectively with patients to help them to understand

**Provide choice to patients (A3)**

* Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of their care
* Respect patients’ decisions to restrict the disclosure and/or use of information
* Explain the implications of disclosing and not disclosing

**Improve wherever possible (A4)**

* Be aware of the issues surrounding confidentiality and seek training or support when uncertain in order to deal with these appropriately
* Report possible breaches or risk of breach

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

## Practice privacy notices

The [practice privacy notice](https://practiceindex.co.uk/gp/forum/resources/privacy-notice-practice.1791/) 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.

Other privacy notices are provided for the following:

* [Children](https://practiceindex.co.uk/gp/forum/resources/privacy-notice-children-england.1794/)
* [Employee](https://practiceindex.co.uk/gp/forum/resources/privacy-notice-employee-england.1793/)
* [Candidates applying for work](https://practiceindex.co.uk/gp/forum/resources/privacy-notice-candidates-applying-for-work.1792/)

## Data Security and Protection Toolkit (DSPT)

Our organisation will undertake the DSPT assessment to demonstrate that the organisation 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.

To demonstrate compliance, our organisation is required to submit the assessment by 31 March annually and use the [DSPT assertions action plan for GPs](https://www.dsptoolkit.nhs.uk/News/Attachment/579) and the DSPT staff [awareness questions](https://www.dsptoolkit.nhs.uk/Help/staff-awareness-questions) for the 2021/22 standards to ensure the practice achieves a successful outcome for the assessment.

Further information is available within the [DSPT Toolkit Guidance](https://practiceindex.co.uk/gp/forum/resources/data-security-and-protection-toolkit-guidance.1045/) and [UK GDPR Policy](https://practiceindex.co.uk/gp/forum/resources/uk-gdpr-policy.1703/).

## Audit

With the advances of technology in healthcare, it is imperative that access is monitored and controlled in an effectual manner. Regular audits must therefore 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 our organisation 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 B](#_Annex_B_–_1) and [Annex C](#_Annex_B_–).

## 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 is available at [Annex D](#_Annex_C_–) that can be used to promote staff understanding and their employee responsibilities when maintaining confidentiality
* A poster is at [Annex E](#_Annex_E_–) which can be used within the organisation or on the practice website to advise patients that at our organisation we will ensure that their confidence will not be compromised if needing to discuss personal information that may be overheard.

# Confidentiality in practice

## Good practice

The following actions at our organisation 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
* 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. The [Smartcard Policy](https://practiceindex.co.uk/gp/forum/resources/smartcard-policy.1110/) 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](https://practiceindex.co.uk/gp/forum/resources/confidential-waste-policy.1585/)
* Staff will not talk about patients or discuss confidential information in areas where they may be overheard

The [Communications Policy](https://practiceindex.co.uk/gp/forum/resources/communication-policy.1008/) provides advice on disclosing information electronically or via telephone to a patient, proxy or third party.

The NHS Code of Practice 2003 is detailed above at [Section 5.2](#_NHS_Confidential_Code).

## Confidentiality breach

Any breach of confidentiality must be reported to the Information Governance Team. All breaches will be recorded and managed in accordance with the Information Commissioners Office (ICO) requirements.

This is further discussed in detail within the [UK GDPR Policy](https://practiceindex.co.uk/gp/forum/resources/uk-gdpr-policy.1703/).

## 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.

# Disclosure

## Disclosing information

The following list describes circumstances when information can be disclosed:4

* When effectively anonymised in accordance with the Information

Commissioner’s Office Anonymisation Code of Practice

* 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 then inform and obtain the approval of the Caldicott Guardian

* 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](https://www.legislation.gov.uk/ukdsi/2002/0110398904/data.htm), obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority1. This is referred to as approval under s251 of the [NHS Act 2006](https://www.legislation.gov.uk/ukpga/2006/41/contents)
* 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 then inform and obtain the approval of the Caldicott Guardian
* 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 then inform and obtain the approval of the Caldicott Guardian
* The patient both has the capacity to consent and consents to the disclosure. Further reading can be sought within the [Consent Guidance](https://practiceindex.co.uk/gp/forum/resources/consent-guidance.707/)
* It is a legal requirement to disclose certain communicable diseases. The full list of these notifiable diseases can be sought at Annex L to the [Infection Prevention and Control Policy](https://practiceindex.co.uk/gp/forum/resources/infection-prevention-control-policy-ipc.700/)

# Summary

Confidentiality compliance will be continually monitored and any findings and subsequent recommendations will be discussed with staff.

It is important that all staff at our organisation are conversant and comply with all matters concerning confidentiality. Failure to do so could have far reaching effects on the confidence that patients have in the practice staff and their relationship with health professionals.

Additionally, all staff must understand the importance of being aware of the action to be taken if they receive a request for information from third parties and the procedure to follow in the event that they wish to make a protected disclosure (whistleblowing).

Signing the agreement at [Annex A](#_Annex_A_-) highlights to the individual the possible outcomes and effects that failure to comply could have on the organisation and the potential of the individual to acquire a criminal record.

All staff are aware of the Caldicott principles and that they have a duty to ensure they always remain compliant as confidentiality is the basis of trust between the patient and this organisation. All staff must ensure that they are aware of their individual responsibilities and their duty to always maintain patient confidentiality.

Any questions relating to this policy should be directed to our Strategic Business Manager in the first instance.

# Annex A – Confidentiality and non-disclosure agreement

I \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ confirm that I have read and understand the Confidentiality and Non-Disclosure Policy and agree to abide by it.

I understand that any breach of this agreement could result in our organisation 's sensitive and confidential data being disclosed to the public or other interested parties and may result in my summary dismissal under the organisation’s disciplinary procedure.

Furthermore, any such conduct on my part which results in an unauthorised disclosure of confidential personal data may render me liable to being reported to the Information Commissioner’s Office (ICO). The ICO may, in turn, institute criminal proceedings against me and, if I am found guilty by a court of law, I could be fined and this may also result in a criminal record.

Signed:

Name (printed):

Date:

# Annex B – 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

Our organisation 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 quarterly basis, and reports produced and retained for assurance purposes.

**Assurance required**

The table overleaf explains the criteria, assurances and evidence required for confidentiality audits. It can be used to assist with ensuring that the organisation and its staff are compliant in data security and protection. It is a useful tool when carrying out an audit of confidentiality as per the Data Security and Protection Toolkit.

**Report template**

[Annex C](#_Annex_B_–) gives an example of a confidentiality report template.

|  |  |  |  |
| --- | --- | --- | --- |
| **Level** | **Criterion for confidentiality audit** | **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 |

|  |  |
| --- | --- |
| **Staff** | **Date audited** |
| Spot check that staff understand their responsibility towards data security |  |
| Spot check that staff are aware of data protection policies |  |
| Have staff received training on data protection? |  |
| Have any staff undergone disciplinary action in relation to data protection and security? |  |
| Spot check that staff understand how to report security breaches and near misses |  |
| **Physical access to hardcopy records** |  |
| Check that the record of which staff have access to areas is up to date |  |
| All offices, files or cabinets which contain confidential information are kept locked when not in use |  |
| Has all confidential waste been disposed of securely and are there destruction certificates? (If applicable) |  |
| Has anyone inappropriately accessed, or attempted to access, confidential records? |  |
| **Digital access to records** |  |
| Is the allocation of administrator rights restricted? |  |
| Have staff access rights been reviewed? |  |
| Check if there is any evidence of staff sharing access rights |  |
| Screens are locked when not in use and smartcards removed |  |
| Check that the password policy is being followed |  |
| Has anyone inappropriately accessed, or attempted to access, confidential records? |  |
| Have appropriate security measures been applied to all computers, laptops and mobile devices? |  |
| Staff are using computers appropriately, e.g., no personal use, no downloading unapproved software, no social media use etc. |  |
| **Sharing data** |  |
| Procedures for safely sharing personal information via post are being followed |  |
| Procedures for safely sharing personal information via fax are being followed |  |
| Procedures for safely sharing personal information via secure email are being followed |  |
| **Legal checks** |  |
| The information asset register has been reviewed and signed off |  |
| The record of processing activities has been reviewed and signed off |  |
| Records of consent are up to date and still applicable |  |

# Annex C – Example of an audit report template

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| [Insert practice name] | | Date of audit: | | | Audit reference no: [01/22] |
| Page [1] of [2] |
| **Summary of audit:** | | | | | |
| **Name of auditor(s):** | | | | | |
| **Date audit conducted:** | | | | | |
| **Date audit closed:** | | | | | |
| [Insert practice name] | Date of audit: | | | | Audit reference no: [01/22] |
| 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: | | |

# Annex D – Confidentiality quiz

**Scenario 1:**

A male patient finishes his consultation with the ANP and, as he is leaving, he asks the reception team if it is OK for him to pick up his 16-year-old daughter’s prescription.

How do you respond?

Could there be any medication that the daughter may not want her father to see?

You are not permitted to let the patient collect his daughter’s prescription without her explicit consent. You have a duty to protect confidential information.

There may be contraception medication that the daughter does not want her father to know about.

**Scenario 2:**

A 15-year-old girl has attended a GP appointment for a review of her asthma. During the consultation she asks the GP for advice about oral contraception and, when questioned about sexual activity, she advises that she is sexually active but has not told her Mum or Dad.

Can the GP breach her confidence and, if so, why?

Yes, on child protection/safeguarding grounds. However, if the GP deems the patient has shown maturity and fully understands the consequences of her request and subsequent actions, her confidence should be upheld.

**Scenario 3:**

You work in a rural practice and it is a very close-knit community with everyone helping one another. You notice your neighbour in the waiting room and after his appointment he appears upset and leaves without saying anything.

Can you check his clinical record to see if there is anything you can do to help?

No, as you have no legitimate purpose for doing so. If you were to search their record this would constitute a breach of confidentiality and a breach of the [Data Protection Act 2018](https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted).

**Scenario 4:**

You have arranged for a patient to collect a printed copy of their medical notes for an insurance matter. You are off to lunch in five minutes and decide to leave the notes (not in an envelope) on the reception desk.

Is this appropriate?

No, you are failing to protect against improper disclosure and this goes against the [NHS Code of Practice 2003](https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice). Leaving the notes in such a position means they would be visible to other staff members and patients. You must never leave patient confidential information in an unsecured area at any time.

**Scenario 5:**

A male patient aged 14 attends the practice and asks for a copy of his medical records.

How do you respond?

Patients under the age of 16 are entitled to see or be given a copy of their records if they have the competence to understand the nature of the request. However, they need to be deemed Gillick competent and, as such, need to be assessed by a healthcare professional before being given a copy of their notes.

**Scenario 6:**

You are handing over to your colleague at reception who is covering your lunch break. You tell them that earlier in the morning you were advised that a patient who had been with the practice for 55 years had passed away.

You wanted to let them know as you knew they had known the patient for a long time.

Is it OK to do so?

Staff do need to know of deceased patients as this prevents unnecessary phone calls being made or letters being sent thereby causing further upset to the family of the deceased. However, staff must not talk about patients or confidential information in areas where they may be overheard.

**Scenario 7:**

You answer the phone and the caller asks for the results of their latest cholesterol test.

What do you need to do?

You should ask the patient to confirm their name, address and date of birth. You can also ask them when they had the test done. Additionally, you could ask further questions to confirm the ID of the caller such as when they were last in the practice before their blood test appointment.

This helps you to ascertain whether it is the patient calling or if it is someone else. If there is any doubt, tell the caller you will ring them back.

**Scenario 8:**

Your practice is holding a group consultation for diabetic patients and this is the first group consultation at your practice. The ANP calls from the meeting room upstairs and asks you to send the six patients who are waiting.

How do you do this?

All six patients would have consented to attend a group consultation but there will be other patients in the waiting room and you need to protect the confidentiality of the patients. So, rather than saying ‘those who are here for the diabetic clinic, please proceed to the meeting room’, you could say, ‘all patients here for the group consultation, please proceed to the meeting room’.

You have called no names out nor disclosed what the group consultation is about and have therefore maintained confidentiality so far as is reasonably practicable.

**Scenario 9:**

You take a call from patient who wants to confirm their appointment with the visiting mental health nurse but it is a really bad line.

What do you do?

Option A: Try to confirm the patient’s details including name, date of birth, address and who their appointment is with by repeating this information to the patient.

Option B: Advise the patient that they need to call back as you are unable to hear them.

Option B – If you were to repeat everything, all the patients in the waiting area may hear you and they would know the patient’s personal details and also that they had mental health issues.

**Scenario 10**

The father of an eight-year-old patient pops into the practice and asks for a copy of the child’s vaccination record as they are going travelling for a month in the summer. You know the parents are divorced and the child lives with Mum.

Can you give Dad a copy of the vaccination record?

Parents do not lose parental responsibility if they divorce or separate and you should allow both parents reasonable access to their children’s health records. The practice does not have to seek consent from the other parent, nor tell the other parent that they have received the request.

NB – Parental responsibility can be restricted by the courts.

1. [NHS E Confidentiality Policy](https://www.england.nhs.uk/wp-content/uploads/2019/10/confidentiality-policy-v5.1.pdf) [↑](#footnote-ref-1)
2. [Network DES Contract specification 2021/22](https://www.england.nhs.uk/publication/network-contract-des-specification-2021-22/) [↑](#footnote-ref-2)
3. [The Information Governance Review (Information: To share or not to share?)](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf) [↑](#footnote-ref-3)
4. [NDG - Caldicott Guardian guidance v1.0](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1013756/Caldicott_Guardian_guidance_v1.0_27.08.21.pdf) [↑](#footnote-ref-4)
5. [ICO About the DPA 2018](https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/#:~:text=The%20DPA%202018%20sets%20out%20the%20framework,protection%20law%20in%20the%20UK.&text=It%20also%20sets%20out%20separate,Information%20Commissioner's%20functions%20and%20powers.) [↑](#footnote-ref-5)
6. [BMJ](https://www.bmj.com/content/336/7649/888) [↑](#footnote-ref-6)
7. [NHS Digital’s operational guidance document A6.1: What is Confidential Patient Information?](https://digital.nhs.uk/services/national-data-opt-out/operational-policy-guidance-document/appendix-6-confidential-patient-information-cpi-definition) [↑](#footnote-ref-7)
8. [NHS E Confidentiality Policy](https://www.england.nhs.uk/wp-content/uploads/2019/10/confidentiality-policy-v5.1.pdf) [↑](#footnote-ref-8)
9. [CQC - About us](https://www.cqc.org.uk/about-us) [↑](#footnote-ref-9)