Policy Name: Caldicott & Confidentiality Policy
Policy Number: 60

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]

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

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.

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 Chorley Surgery 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 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This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time.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. 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.

Who it applies to

This document applies to all employees of the surgery 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

[1] NHS E Confidentiality Policy

but who are working under the Additional Roles Reimbursement Scheme (ARRS)[2].

Why and how it applies to them
This policy outlines the principles that are to be adhered to by all staff at The Chorley Surgery 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 relates to the affairs of the surgery. 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 Chorley Surgery and after the termination of their employment with the practice, observe strict confidentiality and non-disclosure in respect of any information held by the surgery, except when required or authorised to disclose such information by the practice or by law.

The reputation and continuing ability of the surgery 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 surgery 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 The Chorley Surgery and the individual. We will therefore take the appropriate disciplinary action against any employee who commits a breach of confidentiality by reporting it to our Data Protection Officer (DPO).

If it is a serious breach, the DPO will be bound to recommend that it is reported to the Information Commissioner's Office (ICO) who may, in turn, institute criminal proceedings against the individual and, if found to be negligent, the surgery itself. The individual, if found guilty, will be required to pay a fine and acquire a criminal record and The Chorley Surgery 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 in respect of any malpractice or unlawful conduct.

2 The Caldicott principles are derived from the Dame Fiona Caldicott Information

[2] Network DES Contract specification 2021/22

Governance Review in 2013[3] which now forms the current Caldicott Guardian guidance that was published in September 2021 from the National Data Guardian (NDG)[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)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Public Interest Disclosure Act 1998
- Caldicott review: Information: to share or not to share? The Information Governance Review
- The Health and Social Care (National Data Guardian) Act 2018
- Data Protection Act 2018
- Caldicott Principles: A consultation about revising, expanding and upholding the principles (2020)
- The Caldicott Principles (December 2020)
- National Health Service Act 2006
- EU General Data Protection Regulation 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 (2021)
- Records Management Code of Practice (2021)
- Gender Recognition Act 2004

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".*

3 **Definition of terms**

[3] The Information Governance Review (Information: To share or not to share?)
[4] NDG - Caldicott Guardian guidance v1.0

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 (DPA18).

Confidentiality
The principle of keeping secure and secret from others, information given by or about an individual during a professional relationship[5]

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[6] and is also defined within the National Health Service Act 2006 and is also defined within the National Health Service Act 2006.

Protected disclosure
The protected disclosure of unlawful conduct, malpractice or wrongdoings within the organisation is commonly known as "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.[7]

Special Category data
The UK GDPR singles out some types of personal data as likely to be more sensitive and gives them extra protection. These additions are called special category data and the special categories can be found in the ICO document titled What is special category data.

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

[5] BMJ
[6] NHS Digital's operational guidance document A6.1: What is Confidential Patient Information?
[7] NHS E Confidentiality Policy

care organisations and when such information is shared with other organisations and between individuals, both for individual care and for other purposes.

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 The Chorley Surgery 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 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 (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.[8]

Data security and protection toolkit (DSPT)
The NHS Data Security and Protection Toolkit is an online self-assessment tool that enables The Chorley Surgery 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.

Gender Recognition Act 2004
The Gender Recognition Act (GRA) 2004 contains specific guidance on how information about a patient's trans status can be shared.

Gender recognition Certificate
After a minimum of two years and if certain key criteria are met, some trans people can apply for a Gender Recognition Certificate (GRC) under the GRA. If granted,

[8] CQC - About us

the person acquires all the legal rights and responsibilities of their new gender and can obtain a new birth certificate.

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 Chorley Surgery and by each individual working on behalf of the practice. 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 Chorley Surgery, 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 Chorley Surgery.

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 Chorley Surgery 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 Chorley Surgery, 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

Protected information under the Gender Recognition Act

Section 22 of the GRA 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 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.

Section 22 therefore is a privacy measure that prevents officials from disclosing that a person has a trans history.

However, there are exemptions from Section 22 for medical professionals. Statutory Instrument 2005 No.635 (Section 5) advises that it is not an offence to disclose information, 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.

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 as yet meet the eligibility criteria.

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. 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.

Pride in Practice has advised that it should be noted 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 can have serious and unforeseen consequences in 'outing' trans people.

Further reading on GRC and how one can be applied for can be found on Gov.uk here.

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 surgery 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 Andrea Trafford, Business Manager.

The manager will then discuss the request with the partners and consider asking for assistance from the press information/media officer, Jonathan Bridge (jonathan.bridge@nhs.net) at the ICS/CCG.

Whistleblowing or protected disclosures
In respect of any malpractice or unlawful conduct, any employee is entitled to submit a protected disclosure under the surgery 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 Chorley Surgery Whistleblowing Policy provides a procedure for making protected disclosures. This states that protected disclosures are normally made to Andrea Trafford, Business Manager. 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 at Chorley & South Ribble CCG is Paul Richardson, Paul.richardson9@nhs.net to whom concerns may be expressed.

Refer to the Whistleblowing Policy and Procedure

Confidentiality and non-disclosure agreement
All persons engaged to work for and on behalf of The Chorley Surgery 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 Chorley Surgery will also be expected to sign a confidentiality agreement and this document also incorporates fire safety and risk awareness for visitors.

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 The Chorley Surgery, 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.

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 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 The Chorley Surgery is Dr Jo Magapu, GP Partner.

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.

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.

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.

General Compliance
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 Dr Jo Magapu]. The patients of The Chorley Surgery 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 The Chorley Surgery are to adhere to the principles of confidentiality outlined in the NHS Confidentiality Code of Practice 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 The Chorley Surgery are to be informed of the intended use of their information.

The main headings within the Code of Practice are:

Protect patient information (A1)
Protect the patient's information through several 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

The Chorley Surgery 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 Dr Jo Magapu immediately.

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

Data Security and Protection Toolkit (DSPT)
The Chorley Surgery 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, The Chorley Surgery is required to submit the assessment by 31 March annually.

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

Additional compliance tools
In addition to audit, there are further tools that we will embed:

- All members of the organisation will undergo annual confidentiality training
- A confidentiality quiz will be used to promote staff understanding and their employee responsibilities when maintaining confidentiality
- A poster will be used within the organisation and on the practice website to advise patients that we at the Chorley Surgery will ensure that their confidence will not be compromised if needing to discuss personal information that may be overheard.

Good practice
The following actions at The Chorley Surgery 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

- Confidential waste is shredded or disposed of appropriately

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

Confidentiality breach
Any breach of confidentiality must be reported to Andrea Trafford, Business Manager. All breaches will be recorded and managed in accordance with the Information Commissioners Office (ICO) requirements.

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.

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, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority[1]. This is referred to as approval under s251 of the NHS Act 2006

- In child protection proceedings if it is considered that the information required is in the public's or child's interest. In this situation, staff must discuss the matter with

their line manager or Information Governance staff before disclosing who will 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

- It is a legal requirement to disclose certain communicable diseases.

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 The Chorley Surgery] 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 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 Dr Jo Magapu in the first instance.

Annex A – Confidentiality and non-disclosure agreement

To be signed by all individuals employed or otherwise engaged by The Chorley Surgery.

I _____(full name) 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 The Chorley Surgery'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: