**Finney Lane Surgery**

**Finney Lane, Heald Green, Stockport, Cheshire, SK8 3JD.**

**Tel: 0161 983 9000**

# Confidentiality Policy

## Introduction

This policy outlines the confidential nature of patient information and provides guidance to Practice staff on the disclosure of this information.

## Confidentiality

It is vital for the proper care of individuals that detailed records are kept of their medical history and that those concerned with their care have ready access to this information. It is also important that patients can trust that personal information will be kept confidential and that their privacy is respected.

All staff have an obligation to safeguard the confidentiality of personal information. This is governed by law, contracts of employment and, in many cases, professional codes of conduct. A statement of duty of confidentiality is signed by all work experience students and visiting staff who have access to personal information whilst at the Practice.

All staff should be aware that breach of confidentiality could be a matter for disciplinary action and provides grounds for a complaint against them.

## Disclosure of Information to Third Parties

It is understood that information will need to be shared between providers of care for patients to receive efficient and appropriate treatment and support. It is neither practical nor necessary to seek an individual's explicit consent each time information needs to be shared or passed on in this way.

Version 1 – created Sept 2015
Review history – reviewed last July 2024
Next review due – July 2025

Therefore, as long as the patient is aware of what information is to be shared with whom and of their right to refuse then implied consent can be assumed. If an individual does not consent to information about themselves being shared in this way, the individual's wishes should be respected unless there are exceptional circumstances. Every effort should be made to explain to the individual the consequences of their refusal for care and planning but the final decision should rest with the individual.

Clarity about the purpose to which personal information is to be used is essential and only the minimum identifiable information necessary to satisfy that purpose should be made available. Access to personal information should be on a need-to-know basis. In situations which require the provision of patient information to other care providers it is important that all information necessary to ensure full and effective treatment is passed on.

The principles of confidentiality apply equally to all patients, regardless of age. Young people are equally as entitled to confidentiality as all other patients. This means that 16 and 17 year-olds, as well as those under 16 who are 'Gillick competent', can been seen by a doctor/nurse, consent to treatment and expect that this and other medical information about them will be kept confidential, even from their parents, unless they consent to this information being shared. This applies equally to all treatments, including contraception and abortion. A 'Gillick competent' child is one who can understand fully the options available to them and the consequences of each one. More guidance on this can be found in the Consent Protocol.

**Sharing Patient Information**

Sharing of patient-identifiable information is governed by the 6 Caldicott Principles

1. Justify the purpose(s)
2. Don't use patient-identifiable information unless it is absolutely necessary.
3. Use the minimum necessary patient-identifiable information
4. Access to patient-identifiable information should be on a strict need-to-know basis
5. Everyone with access to patient-identifiable information should be aware of their responsibilities
6. Understand and comply with the law

Version 1 – created Sept 2015
Review history – reviewed last July 2024
Next review due – July 2025

All staff are aware of these principles and of their legal obligations.

Staff are also provided with examples of best practice methods for secure transfer of confidential information. This includes (but isn't limited to):

- verbal permission must be obtained from the patient before divulging information - in certain cases, written consent should be obtained
- the patient must be clear to whom information will be given and why, and that they have the right to withdraw consent after it has been given
- verbal permission must be documented in the patient's medical record
- written permission must be filed or scanned into the patient's notes
- if a patient requests that certain information be kept from their family or friends this request must be respected

**Gender Recognition Act 2004**

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 Gender Recognition Act (GRA) 2004. If granted, the person acquires all the legal rights and responsibilities of their new gender and can get a new birth certificate.

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. "Protected information" is defined in Section 22(2) as information relating to a person who has applied for a gender recognition certificate 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. Section 5 of Statutory Instrument 2005 No.635 provides an exemption that applies to: registered medical practitioners, dentists, pharmaceutical chemists, nurses, paramedics, operating department practitioners and trainees in these professions. The following circumstances must apply:

1. The disclosure is made to a health professional.
2. The disclosure is made for medical purposes; and

3. The person making the disclosure reasonably believes that the subject has given consent to the disclosure or cannot give such consent.

All the above must apply.

Patients should never be asked to produce a GRC to 'prove' their trans status. Trans people are not required to obtain a GRC: many simply choose not to 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 above to all disclosures of information about the trans status of a patient; it may not be accurately known whether the person has a GRC or not.

In addition, the general protocols on medical confidentiality and information governance apply to all patients whether they have a GRC or not. Good information governance around this is essential because unlawful and unwarranted disclosures of a person's trans status leave GPs open to legal proceedings and can have serious and unforeseen consequences in 'outing' trans people.

**When Information can be Disclosed without Consent**

The Mental Capacity Act allows for the creation of certain positions, such as a Lasting Power of Attorney, a Court of Protection-appointed deputy or an Independent Mental Capacity Advocate, who assume the responsibility of discussing and agreeing upon healthcare decisions for a patient who is incapacitated. In these instances, certain aspects of the patient's records must be shared to ensure an informed decision can be made. However, only information relevant to the treatment being proposed can be shared and should the patient have expressed a wish that the information remain confidential – whether generally or from a specific person/group – then this must be respected. The same applies to carers, friends or family involved in healthcare decisions on behalf of an incapacitated person, but consideration should be given to exactly how much information is necessary and the potential sensitive or harmful nature of the information.

Anonymous data can be used without a patient's consent, but if data used for research or education makes a patient in any way identifiable then explicit consent must be obtained from the patient for its use.

There are some circumstances in which consent may not be acquired – see the later section on Care. Data.

Version 1 – created Sept 2015
Review history – reviewed last July 2024
Next review due – July 2025

Some legislation sets out a legal requirement that patient information be disclosed in certain circumstances, for example where information could help in the prevention, detection or prosecution of serious crime. Such legislation includes the Road Traffic Act (1988), the Children Act (1989) and the Terrorism Act (2000).

Patient consent is also not needed if it is deemed to be in the public interest or in an individual's vital interest to release certain information, for example if a patient has contracted an infectious disease which might pose a public health risk.

In all cases where consent is not needed, it is still advisable to inform the patient unless this could prove harmful in some way.

The decision to release information in the exceptional circumstances detailed above should be made by a senior member of staff and it may be necessary to seek legal advice. Any situation in which there is doubt over whether or not to disclose patient information without consent should be referred to Medical Defence for consideration and legal counsel.

In all cases where there is a potential public interest in releasing information, consideration should be given to the potential harm of with-holding the information to protect confidentiality and the potential harm – both to the patient in question and the public trust in the NHS – which disclosure may cause. For guidance on issues of confidentiality in relation to safeguarding patients who may be at risk of harm, please see the *Safeguarding Children Policy* or the *Safeguarding Adults Policy* as appropriate.

There are also some statutory restrictions on the disclosure of information relating to AIDS, HIV and other sexually transmitted diseases, assisted conception and abortion. In these situations, advice should be sought.

Where information on individuals has been aggregated or anonymised, it should still only be used for justified purposes. Care should be taken to ensure that individuals cannot be identified from this type of information as it is frequently possible to identify individuals from limited data e.g. age and post code may be sufficient.

Version 1 – created Sept 2015
Review history – reviewed last July 2024
Next review due – July 2025

Any loss or incorrect disclosure of confidential information must be reported to the

Information Governance Lead, and the patient concerned should be informed of the situation.

**Data Protection**

The Practice not only has a responsibility to ensure that confidential information is shared appropriately and legally, but also to maintain adequate security for that information, protecting it against unauthorised access, unlawful processing and loss or destruction.

- all staff will be given guidance on ensuring that confidential information is dealt with as securely as possible
- the Practice will take all reasonable care to protect the physical security of information technology and the data contained within it
- all data stored electronically will be backed up regularly and the backup tapes will be stored in a secure location
- any issues raised about the security of information will be addressed promptly
- any significant events involving breach of confidentiality or data protection will be reported, and measures will be taken to prevent the same circumstance from arising again
- all information systems will be password protected
- all personal files must be kept secure

See also the *Information Governance Policy*.

**Care data.**

Care data is a government initiative which will extract patient data from GP records and store it in a centralised location (the Health and Social Care Information Centre), from where it will be released to third parties for purposes including planning of service provision and medical research. These third parties may include service providers, commissioners, researchers and private companies. In most instances the data will be provided in aggregate, anonymised or potentially identifiable form, but there will be instances in which identifiable data is released

– this will only occur where the patient in question has given explicit consent or there is a legal basis for doing so.

All patients have the right to opt out of this scheme, which will begin data extractions in Autumn 2014. In order to opt out, patients are asked to submit their request in writing to the practice – opt out codes (9Nu0 – to prevent confidential data leaving the GP practice – and 9Nu4 – to prevent other confidential data, such as that from hospitals, leaving the PCSE) will then be added to their records and their written request scanned into their medical notes.

For further guidance, see the *NHS Confidentiality Code of Practice*.

Other relevant Policies include Access to Medical Records Policy, Consent Protocol, Information Governance Policy, Child Protection Policy and Safeguarding Adults Policy.

**Privacy Notice - NHS Digital (Data Provision Notice)**

| | |
|---|---|
| NHS Digital is the secure haven for NHS patient data, a single secure repository where data collected from all branches of the NHS is processed.<br><br>NHS Digital have the power under the Health and Social Care Act 2012 (section 259) to issue a Data Provision Notice.<br><br>Recently a Data Provision Notice was issued for Research and Planning. This Data Provision Notice is valid from 1st September 2021. | |
| 1**) Data Controller** contact details | Finney Lane Surgery<br>Finney Lane<br>Heald green<br>SK8 3JD |
| **2) Data Protection Officer** contact details | Paul Couldrey<br>Data Protection Officer<br>Info@pcdc.org.uk |
| 3) **Purpose** of the processing | To provide the Secretary of State and others with information and reports on the status, activity and performance of the NHS. The provide specific reporting functions on identified. |
| 4) **Lawful basis** for processing | The legal basis will be: - |

Version 1 – created Sept 2015
Review history – reviewed last July 2024
Next review due – July 2025

| | |
|---|---|
| | Article 6(1)(c) “processing is necessary for compliance with a legal obligation to which the controller is subject.” Complying with the Health and Social Care Act 2012.<br><br>And<br><br>Article 9(2)(g) “reasons for processing for substantial public interest’ |
| 5) **Recipient or categories of recipients** of the shared data | The data will be shared with NHS Digital according to directions which can be found at https://digital.nhs.uk/article/8059/NHS-England-Directions-<br><br>Please also see issued Data Provision Notices: https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/data-provision-notices-dpns |
| 6) **Rights to object** | You have the right to object to the data being transferred and in order to do this you should complete an opt out form and send this to the Practice. |
| 7) **Right to access and correct** | You have the right to access the data that is being shared and have any inaccuracies corrected. There is no right to have accurate medical records deleted except when ordered by a court of Law. |
| 8**) Retention period** | The data will be retained for active use during the processing and thereafter according to NHS Policies and the law. |
| 9) **Right to Complain**. | You have the right to complain to the Information Commissioner’s Office, you can use this link https://ico.org.uk/<br>or calling their helpline Tel: 01625 545 745 (national rate)<br><br>There are National Offices for Scotland, Northern Ireland and Wales, (see ICO website) |

Version 1 – created Sept 2015
Review history – reviewed last July 2024
Next review due – July 2025