WOOSEHILL MEDICAL CENTRE

Confidentiality of Patient Information Policy

Introduction

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

Confidentiality

Whilst 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.

All staff should be made aware that our clinical system Emis Web is auditable so anyone accessing the system as part of their job role must have good reason and in the patient's best interest. The Management Team may perform spot checks on all staff to ensure data security is not being breached.

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.

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 put 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 is able to 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

All staff are aware of these principles and of their legal obligations. They are also provided with examples of best practice methods for secure transfer of confidential information

- 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

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 **National data Op-Out**

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.
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*.

Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. Examples of functions that may be carried out by third parties includes:

- Companies that provide IT services & support, including our core clinical systems; systems which manage patient facing services (such as our website and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services etc.
- Delivery services (for example if we were to arrange for delivery of any medicines to you).
- Payment providers (if for example you were paying for a prescription or a service such as travel vaccinations).

Further details regarding specific third party processors can be supplied on request

Woosehill Practice is compliant with the national data opt-out policy
National Data Opt-Out

It is a service that enables the public to register to opt out of their confidential patient information being used for purposes beyond their individual care and treatment. It was introduced for the health and social care system in England on 25 May 2018.

National data opt-outs apply to a disclosure when an organisation e.g. a research body confirms they have approval from the Confidentiality Advisory Group (CAG) for the disclosure of confidential patient information held by another organisation responsible for the data (the data controller), such as an NHS Trust or GP practice.

The CAG approval is also known as a section 251 approval and refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002.

This means NHS Digital can disclose the information to the data applicant (e.g. research body) with section 251 approval without being in breach of the common law duty of confidentiality.

The public can change their national data opt-out choice at any time via https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/or by calling **NHS Digital contact centre on 0300 3035678 or via the NHS App**

Telephone System Confidentiality

The Practice may record telephone calls received from patients for quality monitoring and training purposes. Patients are made aware of this on our website and the recorded greeting's message on contacting the surgery.

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
Safeguarding Adults Policy

The Data Protection Officer (DPO) services are offered to us by Kent and Medway ICB IG team.
Our GDPR and IG Consultant is Lindsay Blamires - NHS South, Central and West (SCW CSU).

Reviewed January 2026
Next review January 2027