Confidentiality Policy

Introduction

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

Applicability

The policy applies to all employees and partners, and also applies in principle* to other people who work at the practice e.g. self-employed staff, temporary staff and contractors – collectively referred to herein as 'workers'.

*Practices should ensure that workers who are not employees are aware of and agree to abide by this policy in principle. In cases calling for action, and if the worker is an employee of another organisation (e.g. an agency), the worker's employer should also be involved

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 members 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.

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 care data.

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 unauthorized 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 centralized 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 HSCIC) will then be added to their records and their written request scanned into their medical notes.

Gender Recognition Act 2004

The 2004 Gender Recognition Act (GRA) makes it a criminal offence to disclose an individual's transgender history to a third party without their written consent if that individual holds a Gender Recognition Certificate (GRC).

Patients do not need to show a GRC or birth certificate in order for the GRA 2004 to be in effect, so it is best practice to act as though every trans patient has one. This means always obtaining a trans patient's written consent before sharing details about their social or medical transition, sometimes also called gender reassignment, with other services or individuals.

This includes information such as whether a patient is currently taking hormones or whether they have had any genital surgery, as well as information about previous names or the gender they were given at birth. Consent should always be obtained before information relating to the patient being trans is shared in referrals and this information should only be shared where it is clinically relevant, e.g. it would be appropriate when referring a trans man for a pelvic ultrasound but not when referring him to ENT.

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

Schoolacre Surgery