Briefing on Confidentiality, Data protection and Human Rights – Appendix 10

As part of the clinical governance requirement in the NHS pharmacy contract, staff and employees need to comply with legal obligations on data protection and confidentiality, including the Human Rights Act.

This Briefing provides the information that should be read by all staff who should then sign the attached declaration.

Confidentiality

The public expects pharmacists and their staff to respect and protect confidentiality. This duty extends to any information relating to an individual which pharmacists or their staff acquire in the course of their work at the pharmacy. Confidential information includes personal details and details of a person's medication, both prescribed and non-prescribed, and medical history.

This is embodied in the NHS Code of Practice on Confidentiality and the RPSGB Code of Ethics, both of which we must comply with. The key principles from the NHS Code are attached – this should be read by all those working at the pharmacy. The full NHS Code of Practice can be accessed via the PSNC website (**http://www.psnc.org.uk/cg**

In addition there is a common law duty i.e. a general legal obligation on staff at the pharmacy to recognise that the public has the right to expect that information that is entrusted to us is treated in confidence and that their privacy will be respected.

Data Protection

The Data Protection Act 1998 (the 'DPA') aims to promote high standards in the handling of personal information, and so protect the individual's right to privacy.

The DPA applies to anyone holding information about living individuals in electronic format and in some cases on paper. The DPA therefore applies to this pharmacy. To ensure that all staff are aware of requirements, the Information Commissioner has published a fact sheet entitled 'What is the Data Protection Act', the contents of which are set out at the end of this document It should be read by all members of staff.

Human Rights

Article 8 of the Human Rights Act 1998 establishes a right to 'respect for private and family life'. This underscores the duty to protect the privacy of individuals and preserve the confidentiality of their health records. Current understanding is that compliance with the Data Protection Act 1998 and the common law of confidentiality should satisfy Human Rights requirements.

There is also a more general requirement that actions that interfere with the right to respect for private and family life (e.g. disclosing confidential information) must also be justified as being necessary to support legitimate aims and be proportionate to the need

Confidentiality and Disclosure of Information

General Principles

Patient information held by contractors is generally held under legal and ethical

obligations of confidentiality. Patients seeking treatment entrust sensitive information to those who provide their healthcare. They do so in confidence, and have the legitimate expectation that their privacy will be respected, and that their health records will be used by the health service to support their healthcare. Information that can identify individual patients must not be used or disclosed for purposes other than healthcare without the individual's explicit consent, or some other legal basis, such as a robust public interest or legal justification for doing so.

However, patient healthcare does require information to be shared appropriately amongst those who provide that care, as well as the use of anonymised or aggregated data to support the wider functioning of the NHS. Generally, patients who present for care are assumed to consent to the required information sharing between clinicians. Ensuring that patients understand how information may be shared underpins this assumption and is therefore extremely important. Where appropriate, clinical and non-clinical staff may need to discuss consent issues with patients and check patient understanding. This is covered in more detail in the NHS Confidentiality Code of Practice.

Patient Information should only be held, used or shared appropriately and with good reason. Where information identifies individuals, it is likely to be subject to Data Protection Act provisions. Where those individuals are patients, there will be obligations of confidentiality and privacy. Even where there are no apparent legal restrictions on disclosing or permitting access to information, care should be taken to ensure that its use will not result in detriment, whether to individuals, to practices or the wider NHS, unless there is a robust public interest in disclosing information, or a legal basis, such as a request under the Freedom of Information Act.

The standards and constraints that apply to the holding, using and sharing of information are important components of NHS Information Governance. This Code of Practice reflects the NHS Information Governance principles and key standards in relation to the disclosure of, or access to, information. The NHS Information Governance toolkit is available at **www.nhsia.nhs.uk/infogov/igt**. The key governance principles are that:-

(i) Contractors should provide a confidential and secure service for patients;

(ii) Information should only be disclosed or shared by contractors when it is lawful to do so;

(iii) Information should be disclosed or otherwise shared by contractors on a "need to know" basis;

Appendix 10

(iv) Where PCTs need to obtain information from contractors, the minimum necessary information should be determined and the disclosure limited accordingly;

(v) Where, exceptionally, there is a need for PCTs to seek access to or to obtain information beyond that generally required for their day to day business, and where access to patient identifiable information is necessary the process of obtaining such information will be open to audit and appropriate scrutiny – such as by a Strategic Health Authority, NHS auditors, or Caldicott Guardians;

(vi) Where data is required that identifies an individual patient, the patient's consent to that data must be obtained, except in very exceptional circumstances, where it may not practicable to obtain consent.

Even though sharing information for healthcare purposes will be lawful within GMS, PMS or APMS practices, personal medical records should only be accessed within practices on a "need to know" basis, for example, by:-

(i) GPs, who will usually have access to the complete clinical record;

(ii) Other health professionals involved in the care of patients, e.g. nurses and allied health professionals employed by the contractor or other organisations such as the PCT or mental health trusts. In some situations, only a summary of clinical information may be required that relates to a particular aspect of patient care;

(iii) Contractor staff with responsibility for the management of patient records, including security and the transfer and updating of records;

(iv) Health professionals employed by local authorities – e.g. in Care Trusts.

What is the Data Protection Act (DPA)?

The following information is published in a Fact sheet by the Information Commissioner.

The Data Protection Act 1998 seeks to strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information.

The DPA gives individuals certain rights regarding information held about them. It places obligations on those who process information (data controllers) while giving rights to those who are the subject of that data (data subjects). Personal information covers both facts and opinions about the individual.

Anyone processing personal information must notify the Information Commissioner's Office (ICO) that they are doing so, unless their processing is exempt. Notification costs £35 / year.

The eight principles of good practice

Anyone processing personal information must comply with eight enforceable principles of good information handling practice.

These say that data must be:

1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate and up to date;
5. not kept longer than necessary;
6. processed in accordance with the individual's rights;
7. secure;
8. not transferred to countries outside European Economic area unless country has adequate protection for the individual.

The six conditions

At least one of the following conditions must be met for personal information to be considered fairly processed:

1. the individual has consented to the processing;
2. processing is necessary for the performance of a contract with the individual;
3. processing is required under a legal obligation (other than one imposed by the contract);
4. processing is necessary to protect the vital interests of the individual;
5. processing is necessary to carry out public functions, e.g. administration of justice;
6. processing is necessary in order to pursue the legitimate interests of the data controller or third parties (unless it could unjustifiably prejudice the interests of the individual).

Sensitive data

Specific provision is made under the Act for processing sensitive personal information. This includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions.

For personal information to be considered fairly processed, at least one of several extra conditions must be met. These include:

Having the explicit consent of the individual;

Being required by law to process the information for employment purposes;

Needing to process the information in order to protect the vital interests of the individual or another person;

Dealing with the administration of justice or legal proceedings.

Rights under the Act

There are seven rights under the Data Protection Act.

1. **The right to subject access**
   This allows people to find out what information is held about them on computer and within some manual records.
2. **The right to prevent processing**
   Anyone can ask a data controller not to process information relating to him or her that causes substantial unwarranted damage or distress to them or anyone else.
3. **The right to prevent processing for direct marketing**
   Anyone can ask a data controller not to process information relating to him or her for direct marketing purposes.
4. **Rights in relation to automated decision-taking**
   Individuals have a right to object to decisions made only by automatic means e.g. there is no human involvement.
5. **The right to compensation**
   An individual can claim compensation from a data controller for damage and distress caused by any breach of the act. Compensation for distress alone can only be claimed in limited circumstances.
6. **The right to rectification, blocking,**

Appendix 10

erasure and destruction
Individuals can apply to the court to order a data controller to rectify, block or destroy personal details if they are inaccurate or contain expressions of opinion based on inaccurate information.

7. **The right to ask the Commissioner to assess whether the Act has been contravened**
If someone believes their personal information has not been processed in accordance with the DPA, they can ask the Commissioner to make an assessment. If the Act is found to have been breached and the matter cannot be settled informally, then an enforcement notice may be served on the data controller in question.

Criminal Offences

A number of criminal offences are created by the Act and include:

Notification offences

This is where processing is being undertaken by a data controller who has not notified the Commissioner either of the processing being undertaken or of any changes that have been made to that processing.

Procuring and selling offences

It is an offence to knowingly or recklessly obtain, disclose or procure the disclosure of personal information without the consent of the data controller. There are some exceptions to this – for example, where such obtaining or disclosure was necessary for crime prevention / detection. If a person has obtained personal information illegally it is an offence to offer or to sell personal information.

Electronic Communications

The Privacy and Electronic Communications (EC Directive) Regulations 2003 cover, amongst other things, unsolicited electronic marketing communications.

Unsolicited marketing calls should not be made to individual subscribers who have opted out either directly or by registering with the central stop-list, the Telephone Preference Service (TPS), or to corporate subscribers (e.g. companies) who have objected either directly or by registering on the Corporate TPS.

Unsolicited marketing faxes should not be sent to individuals without their prior consent or to any subscriber who has objected, either directly or by registering on the Fax Preference Service (FPS).

Unsolicited marketing emails or SMS should not be sent to any individual subscriber who has not consented unless the email address or phone number was collected in the context of a commercial relationship.

Wholly automated marketing calls, i.e. where a recorded message is played and the recipient does not speak to a human being, can only be made where the subscriber concerned (whether individual or corporate) has consented.

The role of the Information Commissioner's Office

The ICO has specific responsibilities for the promotion and enforcement of the DPA.

Under the Data Protection Act, the Information Commissioner may:

- serve information notices requiring data controllers to supply him with the information he needs to assess compliance.
- where there has been a breach, serve an enforcement notice (which requires data controllers to take specified steps or to stop taking steps in order to comply with the law).

Appeals to these notices may be made to the Information Tribunal.

Additional Information

Additional guidance on the Data Protection Act is available on the Information Commissioner website at
www.informationcommissioner.gov.uk

To contact the Information Commissioner helpline please telephone 01625 545745.