Legislation

Data Protection Act 1998 (8 Principles)

There are 8 fundamental Data Protection Principles. The Act regulates the use of personal data. It provides a legal framework that governs the life cycle of information from collection until its final destruction or retention. The Act states that any use of Personal Data should be:

1. Fair and Lawful
2. Used only for specified and lawful purposes
3. Adequate, relevant and not excessive in relation to the purpose for which it was collected
4. Accurate and up to date
5. Not kept longer than is necessary
6. Processed (used) in accordance with the rights of the subject, including their right to access the data
7. Secured against accidental loss, unauthorised disclosure or damage
8. Kept within the European Economic Area

Human Rights Act 1998

Article 8: Everyone has a Right to Respect for his Private and Family Life, Home and Correspondence

Common Law Duty of Confidence

Where information is clearly confidential or has a quality of confidence, you and your staff are obliged by Common Law not to divulge that information, to anyone not authorised to have knowledge of or access to that information.

Sensitive Information Under Your Control

Amongst the most sensitive information held by pharmacies is the information contained on prescriptions. Pharmacies must ensure that when transporting or transferring these items, all reasonable measures and precautions are taken to mitigate, or at the very least reduce the risk of loss, damage or destruction.

Further Information Resources

Family Practitioner Services

Eastern Office: Tel: 028 90 553784
Western Office: Tel: 028 71 860086
Southern Office: Tel: 028 37 414622
Northern Office: Tel: 028 25 311140
Website: www.hscboard.hscni.net

Pharmaceutical Society (PSNI)

Tel: 028 9032 6927

Website: www.psni.org.uk

Information Commissioner (ICO) NI

Helpline: 0303 123 1113

Website: www.**ico**.gov.uk

Data Protection Checklist

- ☐ **Am I registered with the ICO (notification)?**
- ☐ **Do my staff know their responsibilities?**
- ☐ **Have I clear policies and procedures for managing the information I hold?**
- ☐ **Is the patient/client level data I hold secure?**
- ☐ **Do I know what to do if someone asks for a copy of the information I hold about them?**
- ☐ **Do I know what to do in the event that I lose patient/client level data?**

HSC Health and Social Care Board

A guide to the Secure and Confidential Handling of Patient/Client Data in Your Possession as required by the Data Protection Act 1998

Community Pharmacies

Issued by the Health and Social Care Board for Northern Ireland.
Note: all information contained within this guide correct at the time of issue: August 2010.

Photograph courtesy of Pharmacy in Focus

Introduction

As a Data Controller, you and your employees are legally obliged to protect and maintain the confidentiality of personal information in your charge. This responsibility is set out in the Data Protection Act (DPA) 1998 and should be reflected within your staff contracts of employment.

The following principles should underpin your procedures for dealing with Patient level data:

- Provide patients with information that outlines why you need their information and what you will do with it
- Only collect or use patient/client identifiable information when absolutely necessary
- Only pass on identifiable patient/client data in legitimate circumstances
- Only collect the minimum identifiable information required
- Only collect information for one or more specified purposes
- Ensure that access to patient/client level data is restricted within the Pharmacy to a 'Need to Know' basis
- Ensure that **you** and **your staff** know their responsibilities to protect information.
- Complying with the law is an obligation

Statutory Obligations

Notification. You are legally obliged to **notify** your processing of personal data with the ICO; **not to do so is a criminal offence**.

Subject Access Request. Individuals have a legal right to **access** information you hold about them. If you receive a legitimate request, you have 40 days to comply, with limited exceptions. For further information on your statutory obligations, go to www.ico.gov.uk.

Basic Principles

Any personal information collected for one purpose must not be used for another purpose without the consent of the individual unless it is permitted by the Data Protection Act 1998.

A patient's right to confidentiality is protected in law. Patients have a legal right to know what information is being collected, why it is being collected, the purpose for which the information will be used and who it will be shared with.

Patients have a right to request that you stop using their information. Advice should be sought if you receive such a request.

You and your staff are legally obliged to protect information and maintain its confidential nature. Only pass on information once you are assured that the transfer is legitimate.

The Data Protection Act is here to protect both the subject of the data and the person who legitimately uses that data. It should not however be applied so rigidly that it restricts the necessary flow of information for the benefit of the patient or patients.

You are Responsible for the Information Under your Control

Under the Data Protection Act, you, the business owner and employer, are the Data Controller, and as such, you are legally responsible for ensuring that information is used legitimately, transferred legitimately, stored securely and once no longer required, disposed of permanently. If circumstances occur where you are unsure of what you should do, you should seek expert advice before taking any action that involves personal information in your care.

Duty of Care

All reasonable care should be taken to protect the physical security of personal information from accidental loss, damage, destruction, unauthorised access, unlawful processing or accidental disclosure.

Good practice:

- Password protect all computers and keep passwords safe.
- Consider installing encryption software on computers and electronic devices.
- Patient/client information should be kept secure and not left unattended.
- Faxing is not secure. Personal data should not be faxed except where there is no alternative and there is an overriding clinical need.
- Envelopes containing personal data must be secured whilst in transit. We recommend that you consider purchasing 'Special Delivery' when sending information via Royal Mail.
- Always check the authenticity of a caller before divulging sensitive data.
- Have a records policy that sets out how long certain types of information should be held, and what happens to it once it has passed its retention period.
- Develop robust policies and make sure your staff comply with these.

Data Loss or Breach

It is critical that in the event that you lose information or if its integrity is compromised, you manage the incident quickly and effectively. You should also contact the HSCB and inform them immediately of the incident. For further information go to www.ico.gov.uk.