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.

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.

Further Information Resources

Family Practitioner Services

Belfast Office: Tel: 028 9536 3926

South East Office: Tel: 028 9536 3926

Western Office: Tel: 028 9536 1010

Southern Office: Tel: 028 9536 2104

Northern Office: Tel: 028 9536 2845

Website: www.hscboard.hscni.net

British Dental Association (NI)

Tel: 028 9073 5856

Website: www.bda.org

Information Commissioner (NI)

Helpline: 0303 123 1113

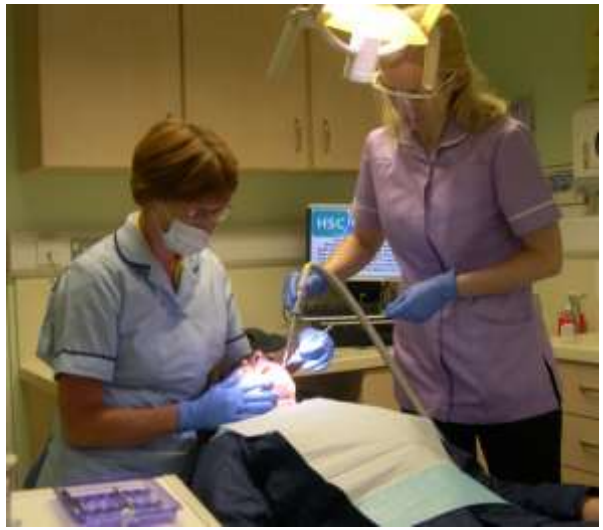
Website: www.ico.gov.uk

Data Controllers Checklist

- ☐ **Am I registered with the ICO (notification)?**
- ☐ **Do my staff know their responsibilities?**
- ☐ **Have I clear policies and procedures for managing and protecting the information I hold?**
- ☐ **Is the patient/client level data (both in physical and electronic format) 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



Dental Providers

Issued by the Health and Social Care Board for Northern Ireland. Note: all information contained within this guide correct at time of issue: April 2013 Version 1.1

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 1998 and should be reflected within your staff contracts of employment.

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

- Your patients have a right to expect to have their information held securely and shared appropriately, for example, with other Health Professionals involved in their care. Be prepared to answer any questions they may have about your processes and procedures.
- Ensure that you and the Practice staff understand that a patient has a right to see a copy of the information held by the Practice (see **Subject Access Request**)
- Records generated through the care of a patient, should be accurate, timely and factually correct. An accessible personal health record includes factual information about treatments received as well as medical opinions that have been recorded.
- Ensure that access to patient/client level data is restricted within the Practice to a 'Need to Know' basis.
- Ensure that employees have access to expert opinion when they are unsure how to deal with issues relating to securing information or releasing information if they are requested to do so.
- Complying with the law is a statutory obligation and it applies to all employees.

You may wish to refer to the 'Good Practice Guidance' leaflet titled '***Information Security***' which compliments this leaflet with helpful tips and information that will assist you to meet your legal obligations.

Duty of Care

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

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.

Information under your Control

Under the Data Protection Act 1998, the business owner and employer, is the Data Controller, and as such, is 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.

Social Media and Smartphones

Personal Data can be captured in many formats, including pictures and video footage. With the increasing use of smartphones[1] and social media sites[2], inadvertent breaches of privacy are becoming all too frequent. We recommend that the Practice adopts a social media policy which reminds staff of their duty to maintain confidentiality when using these sites, and also clearly define acceptable use of smartphones by staff within the business premises in respect of picture, audio and video recording.

[1] an internet enabled device with video, audio and photo functionality

[2] a web based internet site where information and/or images are shared (Facebook, Twitter etc)

Statutory Obligations

Notification – Registering your Practice on the Public Register of Data Controllers. If you process personal information, you are legally obliged to register the processing with the Information Commissioners Office. **Not to do so is a criminal offence**. If you wish to speak to someone about registering your Practice, you should call the Information Commissioners (ICO) Helpline on the number below.

Helpline – 0303 123 1113

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.

Good practice:

- 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. The HSCB recommend that you consider purchasing 'Special Delivery' when sending information via Royal Mail.
- Always check the authenticity of a caller before divulging sensitive data.
- Develop robust policies and make sure your staff comply with these.
- Identify a member of staff responsible for Data Protection and Information security and support their training needs.