Legislative Summary: Data Protection in the Healthcare Sector

Making sure it's secure.™

The Data Protection Act (UK)

Enacted: 1998; Into force: 2000 – under Information Commissioner's Office (ICO)

1 What the law covers:

Eight principles governing the:

- Protection of the processing and use of personal data against unauthorised or unlawful use, accidental loss, destruction or damage
- Rules on the processing of personal data including obtaining, recording, holding, organising, adapting, altering, using, disclosing and destroying it

Note: Data protection legislation is currently under review within Europe. This could impact existing health sector policy guidelines and codes of practice to ensure ongoing compliance.

2 What is "personal data":

Information that allows the identification of a living individual – i.e. name, date of birth, address, national insurance number, etc.

3 Who must adhere to the regulations:

Any organisation, business or person who processes personal data including patient contact details, medical history, prescriptions, etc.

For more information:

Information Commissioner's Office – ico.org.uk
Department of Health – dh.gov.uk
Care Quality Commission – cqc.org.uk
General Medical Council – gmc-uk.org

4 DPA and healthcare information management:

There are several key policies and procedural guidelines designed to ensure compliance.

A. Department of Health (DofH) Records Management Code of Practice for the NHS:

- Establishes the information governance framework for NHS records management
- Sets out legal obligations applying to NHS records and minimum retention periods
- Details recommendations on record retention and disposal arrangements

The DofH has also published its own Personal Information Charter, describing its commitment to the protection of personal data.

B. ICO Sector Guides: Health

- Highlights that this sector handles some of the most sensitive personal data
- Covers healthcare Data Protection and Freedom of Information obligations
- Provides advice on data breach reporting requirements

C. Care Quality Commission ("CQC") Code of Practice on Confidential Personal Information:

- Outlines the CQC's role as the independent regulator, ensuring government standards are met by hospitals, care homes and care services
- Details its extensive powers to access documents and records during an inspection
- Covers its policies and practices to protect confidential personal information – that also impact those who work with the CQC

D. General Medical Council ("GMC"):

- Provides additional guidance for confidentiality of patient information – especially its disclosure
- Some private healthcare providers expressly refer to GMC confidentiality guidance, stating their policies comply with both the GMC and DPA

5 How to comply:

Every organisation processing personal data must be registered with the ICO (unless exempt).

Personal data should be processed fairly and lawfully so that the information collected is:

- Restricted to only what is needed for a specific purpose
- Kept secure, relevant and up to date
- Only held for as long as needed
- Available to the subject of the information to see it on request

Organisations are still ultimately responsible for personal data even when using third party "processors", e.g. a shredding company.

6 Offences/penalties for non-compliance:

1. For a serious breach:

- Monetary penalty notice of up to **£500,000**
- Adherence to an Undertaking (a published enforcement notice)

A serious breach, deliberate or negligent, is determined based on the volume of personal data and level of sensitivity.

2. Other criminal offences:

- Processing personal data without being registered as a data controller with the ICO
- Failure to notify the ICO of changes to the data controller's details
- Failure to notify the ICO of changes in the processing of data

Under Section 55, the unauthorised and wilful, or negligent, act of:

- Obtaining or disclosing personal data or the information contained in personal data
- Procuring the disclosure to another person of the information contained in personal data

Penalties:

- Summary conviction: fine of up to £5,000
- Convicted on indictment: **unlimited fine**

The ICO is also seeking prison sentences to further deter unlawful use of personal data.

7 Secure document retention and disposal guidelines:

Overview of ICO guidelines:

- ☐ Train staff on the importance of information rights, and their responsibility for delivering them
- ☐ Keep personal data secure with processes, people and technology
- ☐ Know the information kept, who it is about and where it is stored
- ☐ Securely dispose of personal information as soon as it is no longer required
- ☐ Assess data security and retention policies regularly
- ☐ Minimise the amount of personal data stored

Recommended inclusions for a document retention policy:

- ☐ A statement of purpose
- ☐ Categories of documents and how long they should be kept
- ☐ Definition of "document" and the format and length of time in which it is to be retained (electronic or hard copy)
- ☐ Guidance on creation of documents
- ☐ Members of staff designated to deal with the document management system
- ☐ Methods of document destruction, including those carried out by third parties
- ☐ How to keep an accurate record of documents destroyed

8 How Shred-it can help:

Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organisation's needs

Advice and Expertise

- Trained experts in information security
- Provide a Data Security Survey at your organisation
- Helpful resources available at shredit.co.uk/resource-centre

For peace of mind, contact Shred-it today

0800 028 1164 | shredit.co.uk