Scottish Health Informatics Programme

KEY POINTS YOU NEED TO KNOW ABOUT DATA PROTECTION

(1) Key concepts

The key concepts which underpin the DPA are outlined in s1 and s2 of the Act.

Concept	Definition	Why important?
Data	Information which is, or is intended to be, processed electronically; is recorded as part of a relevant filing system; forms part of an accessible record under s68 (this includes health records); or which is held by a public authority.	In order for the DPA to apply the information must fall within the definition of 'data.'
Relevant filing system	A manual filing system which is structured, whether by reference to individuals or by criteria relating to individuals, in such a way that specific information relating to a particular individual is important.	The DPA only applies to manual data which is held in a 'relevant filing system.'
Personal data	Any data which relates to a living individual who can be identified from those data for from those data any other information in (or is likely to come into) the possession of the data controller.	The DPA only applies to 'personal data.'
Sensitive personal data	Includes information about health, as well as race and ethnic origin	The DPA imposes more stringent conditions on the processing of 'sensitive personal data.'
Processing	The broad definition in the DPA encompasses just about anything that can be done with data.	The DPA applies to the processing for data.
Data subject	The individual who is the subject of personal data.	The DPA gives certain rights to the data subject. The most important of these is the right to subject access in s7-s9.
Data controller	The person(s) who determine the purposes for which and the manner in which data are to be processed.	The data protection principles are obligations which the DPA imposes on data controllers. Under the SHIP framework the Safe Haven will take on the legal responsibilities of the data controller, along with the data custodian.
Data processor	The person(s) who process data on behalf of the data controller.	Although legally it is not the duty of the data processor to comply with the data protection principles, this should be done as a matter of good information governance.

(2) The data protection principles

The data protection principles are contained in schedule 1 of the DPA and set out optimal standards for information handling.

	Principle	What this means?	How to comply?
1	Personal data shall be processed fairly and lawfully and shall not be processed unless, for personal data, one of the conditions in schedule 2 is satisfied and, for sensitive personal data, one of the conditions in schedule 3 is also satisfied.	You must be clear and open about your reasons for processing data and any legal obligations must be satisfied. You must also look to ensure you satisfied at least one condition under schedule 2 and possible also schedule 3.	✓ Comply with schedule 2 and 3 conditions. ✓ Have legitimate grounds for processing data. ✓ Don't use the data in ways that could have an adverse effect on the data subject. ✓ Be clear and open about how you intend to sue data. ✓ Don't do anything unlawful with the data.
2	Personal data shall be obtained only for one or more specified and awful purposes, and shall not be further processed in a manner incompatible with those purposes.	You must be clear about your reasons for obtaining the data. Note the research exemption in s33 (see below).	✓ Be clear about why you are obtaining personal data. ✓ Be clear about what you intend to do with the data.
3	Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.	You must identify and only obtain the minimum amount of personal data needed to fulfil the purpose for which you need the data.	✓ Ensure that the personal data you hold is sufficient for your research purposes. ✓ Ensure that you do not hold more information than is necessary for that purpose.
4	Personal data shall be accurate and kept up to date.	You must ensure that any personal data you hold is accurate and up to date.	✓ Take practical steps to ensure the accuracy of the data you hold. ✓ Consider whether it is necessary to update the data.
5	Personal data shall not be kept for longer than is necessary.	You should have regard to what is a reasonable period of retention for the data. Note the research exemption in s33 (see below).	✓ Review the length of time for which you keep personal data. ✓ Securely destruct data which is no longer required or is out of date.
6	Personal data shall be processed in accordance with the rights of data subjects under the DPA.	You should be aware of the rights of the data subject.	✓ Be aware of what the rights of the data subject are and observe them.
7	Appropriate technical and organisation protections shall be put in place to protect data against unauthorised processing or accidental loss.	You must have appropriate security measures in places to prevent the personal data you hold being accidentally or deliberately compromised.	✓ Design and organise your security mechanisms to fit the personal data you hold. ✓ Be clear about who is responsible for data security.
8	Personal data shall not be transferred to a territory outside the European Economic Area unless that county ensures adequate levels of data security.	Ensure any that any country outside the EEA that you transfer personal data to has adequate data security mechanisms in place.	It is unlikely that you will be transferring any personal data outside the EEA and therefore you should not need to worry about this principle.

(3) Conditions for processing personal data

Under the first data protection principle, personal data shall not be processed unless at least one of the conditions in schedule 2, and in the case of sensitive personal data also schedule 3, is satisfied.

As health data is sensitive personal data, any secondary use of patient data will need to be processed in accordance with at least one condition under schedules 2 and 3.

Personal Data

Relevant conditions:

Condition	What this means?	How to comply?
Consent	Consent must be legally valid, i.e. it must be informed and given voluntarily by a competent individual.	✓ Examine the circumstance of each case to decide whether there is already consent to your proposed data use, or whether consent can practically be obtained.
The 'legitimate interests condition'	This condition is intended to permit processing which is not covered by any of the other conditions. It requires a balancing to be struck between the interests of the data subject and the public interest in the research project.	✓ The data must be processed for your legitimate interests. ✓ These interests must be balanced against the interests of the individual(s) concerned. ✓ The processing must be fair and lawful and must comply with the data protection principles.

Sensitive Personal Data

Condition	What this means?	How to comply?
Explicit consent	This is a higher standard of consent than is required under schedule 2. It requires the individual's consent to be absolutely clear.	✓ Obtain informed, specific and express consent from the data subject to use their personal data.
Processing necessary for medical purposes	The term 'medical purposes' includes medical research. You must show that there is a public interest in your research project.	✓ Demonstrate that there is a public interest in your research project and that this is not overridden by any concerns over confidentiality.
Processing which is in the public interest and necessary for medical purposes	This additional condition is in the Data Protection (processing of Sensitive Personal Data) Order 2000. It provides that sensitive personal data can be processed if the processing is in the public interest, is necessary for medical purposes, doesn't support decisions for any particular data subjects, and is not likely to cause any damage or distress.	✓ Show there is a public interest in your research project. ✓ Show that the processing is necessary for medical purposes. ✓ Show that the research doesn't support decisions for any particular data subject. ✓ Show that the research is not likely to cause any substantial damage or distress.

(4) Rights of the data subject

The rights of the data subject are contained in part II of the DPA.

In practice, the **right to subject access** is the only rights that you are likely to come across in the context of the secondary use of patient data for research purposes.

Right	What this means?	How to comply?
Right to subject access	Entitles the data subject to be informed by the data controller whether they, or someone else on their behalf, are processing the individual's personal data.	✓ The right includes the rights to be given a description of the personal data which is being processed, the purposes for which they are being processed, and to whom the data has been/ could be disclosed to. But- × The 'research exemption' in s33 provides that there is an exemption to the subject access right where data are being processed for research purposes only. This means that you will only have to comply with such a request in certain circumstances, namely, where the rights of your research project are made available in a form which identifies data subjects.

(5) The research exemption

The 'research exemption' is contained in s33 of the DPA. It provides exemptions from certain parts of the DPA where data is being processed for research purposes only.

The exemption applies where:

- The data are not processed to support measures or decisions relating to particular individuals.
- The data are not processed in such a way that substantial damage or substantial distress is likely to be caused to any data subjects.

Exemption	Effect?
For the purposes of the second data protection principle, the further processing of personal data for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which the data was obtained.	If data which has been obtained for the purpose of processing for research purposes is to be further processed for different research purposes, this will be held to be compatible with the purposes for which the data was obtained.
Personal data may be kept indefinitely	The exemption may only be used if research is actually being carried out or if there is a firm intention to use the records for that purpose.
Exemption from subject access requests.	Subject access does not have to be given provided that the results of the research are not made available in a form that identifies that data subject.

(6) Data security

The DPA requires adequate data security provisions to be in place to address the risks of (a) unauthorised or unlawful processing of personal data, and (b) accidental loss or destruction of, or damage to, personal data.

If you are using a SHIP Safe Haven then the Safe Haven will provide you with the necessary data security. However if data is directly transferred to you, then you must consider what data security mechanisms you need to put in place to protect the personal data you are using.

When considering what level of data security you require you should consider:

- The nature of the data;
- The harm which could result from improper use, accidental loss or destruction of the data;
- The nature and extent of your organisations premises and computer systems;
- The number of persons who could have access to the data;
- Any personal data to be held by a third party on your behalf.

You should ensure that you have both physical and technological security and management and organisational security mechanisms in place.

Examples of physical and technological security mechanisms:	**Examples of management and organisational security mechanisms:**
• Technical security measures to protect computerised information. • Ensuring the quality of doors and locks and protecting your premises with alarms and CCTV. • Secure waste disposal. • Keeping portable equipment secure. • Supervising any visitors to the premises. • Encrypting any personal data which is held electronically.	• Building a culture of security and awareness in your organisation. • Identifying an individual who is responsible on a day to day basis for data security. • Establishing a clear process of accountability. • Periodic checks to ensure that your organisation's security measures remain appropriate and up to date. • Training staff to ensure they are familiar with the security measures in place and that they are aware of their responsibilities.