

Data protection and record retention

1 Introduction

This is the second in a series of briefings to assist managers of drug treatment services to develop effective management policies and procedures.

This briefing outlines the background to the Data Protection Act, providing definitions, procedures and defining the eight key principles in relation to information handling. The final section answers frequently asked questions from drug treatment service providers in relation to data protection. This document provides information and general guidance only. It is not, nor is it intended to be, legal advice. It should also be read with reference to briefing number one in this series: *Confidentiality and information sharing*.

2 The Data Protection Act 1998

The Data Protection Act 1998 came into force in March 2000, replacing the Data Protection Act 1984. It sets out a clear regime for processing personal information, applying to paper records as well as those held on computer. The Act represents a major progression in law with regard to how personal information or personal data must be treated. The Act gives private individuals (data subjects) greater control over how their personal information is gathered, used, housed and shared, while requiring those who record and use personal information (data controllers) to be open about how they use this information and to adhere to the data protection principles. Compliance with the Data Protection Act should not be viewed as an additional burden on drug treatment services but as good practice, which protects staff's, volunteers', management committee members' and service users' rights.

The Data Protection Act is based on the fundamental Right of Privacy, as provided for in the European Convention on Human Rights. The recently enacted Human Rights Act 1998 implements the Convention into United Kingdom domestic law. Under that Convention "everyone has the right to respect for his private and family life, his home and his correspondence."

2.1 Definitions

Personal data: This is any information that relates to an identifiable, living individual, that is someone who can be identified from the data and other information in the possession of, or likely to come into the possession of, the data controller. Information that is effectively anonymised is not covered in the Data Protection Act. For drug services personal information could include information held on service users, staff, volunteers and management committee members.

Processing: This is widely defined and includes most activities that could be done with data: obtaining, recording or holding the data, or carrying out any operation(s) on the data.

Relevant filing system: The 1998 Act covers paper filing as well as electronic data. A relevant filing system is defined by the Act as “a set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to certain criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible” (HMSO, 1998). This means that any manual filing system, where personal information is readily available, can be considered to be a relevant filing system.

Data controller: This is the party or organisation who or which, alone or jointly, determines the purpose(s) for which, and manner in which, the personal data is processed. This can be any type of company or organisation, large or small, within the public or private sector. A data controller can be a sole trader, partnership, or an individual.

3 Notification

The Information Commissioner maintains a public register of data controllers in the UK. Most data controllers will need to notify the Commissioner of the purposes of their processing, the personal data processed and the recipients of the data processed. Failure to notify the Commissioner, if required, is a criminal offence. The Commissioner’s website (www.dataprotection.gov.uk) allows visitors to search the register and fill out an on-line self-assessment form to determine whether notification is required. All drug treatment services will need to notify the Commissioner if they hold personal information about service users, staff, volunteers and management committee members. The size of your organisation is immaterial.

Drug services can notify the Commissioner via the data protection website or by phoning the notification helpline on 01625 545 740. For general advice about data protection drug services can ring the enquiry/information line on 01625 545 745 or email data@dataprotection.gov.uk. The annual notification fee is £35. The register website is directly accessed at www.dpr.gov.uk.

4 Data protection principles

There are eight data protection principles, sometimes referred to as the principles of “good information handling”, with which data controllers are required to comply. Non-compliance is not a criminal offence but, if the Commissioner considers that one or more of the principles has been, or is being, breached, enforcement action can be taken. Failure to comply can then become a criminal offence.

The eight data protection principles state that data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept for longer than is necessary
- processed in line with the data subject’s rights
- secure
- not transferred to countries outside the EU without adequate protection.

4.1 First principle: Personal data must be fairly and lawfully processed

In general terms, the first principle requires that data controllers comply with the Fair Processing Code. This means that when obtaining data from data subjects, data controllers must ensure that the following information is made readily available:

- the identity of the data controller
- the identity of any nominated representative for the purposes of the Act

- the purpose(s) for which the data will be processed
- any other information necessary to ensure fairness, such as the likely consequences of the processing, and whether they envisage the data being disclosed to a third party.

Data controllers should be clear about why the information is wanted and should have a legitimate reason for processing it.

Processing can only be carried out where one of the following conditions has been met:

- The data subject has consented to the processing.
- Processing is necessary for the performance of a contract with the data subject.
- Processing is required under a legal obligation.
- Processing is necessary to protect the vital interests of the data subject.
- Processing is necessary to carry out public functions.

Consent is not defined in the Act but as a general rule it should be active – drug services cannot infer consent from a lack of response (e.g. not responding to a letter) but they can infer it from an action (e.g. presenting an arm for a pulse to be taken). To be valid, consent should be informed and freely given. Consent does not need to be written, though a signed consent form, as evidence of consent, is good practice. It is important that all service users are given sufficient information to be able to understand how identifying information might be used and to question and object, if they wish. The Act makes a distinction between personal data and **sensitive personal data** (explained below). Consent for processing sensitive data must be **explicit**. Explicit consent means the data subject must be made aware of the details of the proposed processing, the type of data to be processed and any disclosures.

The Act does allow for the processing of sensitive personal data for medical purposes when carried out by a “health professional or a person who in the circumstances owes a duty of confidentiality, which is equivalent to that which would arise if that person were a health professional” (HMSO, 1998).

Processing sensitive personal data

Personal data considered by the Act to be sensitive data can only be processed under strict conditions. Sensitive data includes:

- racial or ethnic origin
- political opinions
- religious or other beliefs
- trade union membership
- health
- sex life
- criminal proceedings or convictions.

Sensitive data can only be processed:

- with **explicit** consent of the data subject
- if required by law for employment purposes
- to protect the vital interests of the data subject
- for administration of justice or legal proceedings.

Drug treatment services will mostly be processing information of a sensitive nature (e.g. health) and should, in most cases, gain the data subject’s explicit consent to processing.

4.2 Second principle: Personal data must be processed for limited purposes

Personal data must only be obtained for specified purposes and may only be processed in accordance with those purposes.

4.3 Third principle: Personal data must be adequate, relevant and not excessive

Data controllers should ensure that only data needed for the specified purpose of data processing is collected. This means that drug services should not collect data that is not required to meet a service user's needs.

4.4 Fourth principle: Personal data must be accurate

Data controllers must ensure that personal data is kept up-to-date and any mistakes corrected.

4.5 Fifth principle: Personal data must not be kept for longer than necessary

The Act does not define "longer than necessary" but states that personal data must only be held up to the point when the purpose for keeping the data has ceased. Only in exceptional circumstances should data be kept indefinitely. For more detail see section 5. *Record retention*, in this briefing.

4.6 Sixth principle: Personal data should be processed in accordance with the rights of data subjects under this Act

The Data Protection Act gives data subjects greater control over their personal data and how this data is used. The data subject has the right to give or withhold consent to processing their personal data and the right to be informed of any processing actions. The data subject can request access to their personal data. If a drug treatment service charges a fee, it should be no more than £10.

In essence, drug treatment services will have to comply with requests from data subjects for information about their personal data and its processing. They will also need to comply with a justified request from a data subject to cease processing that is likely to cause damage or distress. A written subject access request must be dealt with promptly: 40 days from receipt of letter or 40 days from receipt of additional information or fee, if requested.

A data controller can refuse a data subject's access request when it would disclose information about another identifiable individual, unless the third person has consented or it is reasonable in all the circumstances to comply with the request without their consent (see *Frequently asked questions* section 6.7 below).

It is important that all staff can recognise a data subject access request and realise it must be dealt with urgently. The letter may not mention the Data Protection Act specifically and may just say, "I want to see what information you have on me."

4.7 Seventh principle: Personal data must be kept secure

Data controllers should take "appropriate technical and organisational measures" (HMSO, 1998) to protect against unauthorised or unlawful access to personal data. They should take into account the nature of data and the harm to data subjects if disclosed or lost. Examples of security measures include:

- having passwords on computers, which are changed regularly
- positioning computer terminals so casual callers cannot see the screen
- providing procedures to verify the identity of telephone callers
- having back-up computer files and keeping them securely.

4.8 Eighth principle: Personal data should not be transferred overseas unless within the European Economic Area (EEA) or a country that has adequate data protection principles

If a drug service needed to transfer data to a country outside the EEA (the European Union plus Norway, Iceland and Liechtenstein) it would need to ensure that the receiving country had adequate protection for data or that the data subject had given consent.

5 Record retention

The Data Protection Act states that personal files should not be kept “longer than necessary” but does not define this concept. *Health Service Circular 1999/053: For the record* (Department of Health, 1999) sets out retention periods for NHS records. The guidance states that the length of the retention period depends on the type of record and its importance to the business of the NHS trust or strategic health authority. Generally, case records should be kept for **eight years** after the conclusion of treatment but:

- Children and young people’s records should be kept until the service user’s 25th birthday or 26th if the young person was 17 at the conclusion of treatment.
- The records of “mentally disordered persons” (as defined by the Mental Health Act 1983) should be kept for 20 years after no further treatment was considered necessary; or eight years after the service user’s death, if they died while receiving treatment.
- Where legal action has been commenced, records should be kept as advised by legal representatives.

Data Protection Act 1998: guidance to social services (Department of Health, 2000) suggests that personal files should be kept no longer than six years after the subject’s last contact with the authority, unless there are exceptional circumstances.

Drug services operating the treatment element of drug testing and treatment orders will need to agree locally determined record retention periods with the probation service they are working with. The Probation Service is preparing national guidance on record retention.

Drug services in the voluntary sector should adopt the NHS standards as good practice in the retention of service users’ personal files and to ensure compliance with the Data Protection Act. Voluntary drug services commissioned by statutory services should have compliance with these guidelines included in their contracts.

6 The Freedom of Information Act 2000

The Freedom of Information Act 2000 gives a general right of access to all types of recorded information held by public authorities and those providing services for them, subject to specific exemptions. Public authorities include, for example, national and local government, the NHS (including primary care trusts, GPs and the NTA) and the police. The general right of access to information comes into force in January 2005. In the meantime public authorities must produce a “publication scheme”: a guide to the information they hold that is publicly available. The Information Commissioner is responsible for enforcing the Act and provides further information at www.dataprotection.gov.uk. Additional information and guidance for NHS organisations is available at www.foi.nhs.uk.

7 Frequently asked questions

7.1 Do all drug treatment services need to notify the Information Commissioner?

A service which only kept information on its staff and volunteers, or a non-profit service which only kept information on its management committee, would not be required to notify the Commissioner. They would, however, still be required to comply with the data protection principles. Any service keeping personal data on service users must notify the Information Commissioner and comply with the data protection principles.

7.2 Can drug services still provide monitoring information to DATs and NDTMS (National Drug Treatment Monitoring System)?

The National Drug Treatment Monitoring System (NDTMS) collects data about all service users in ongoing structured care: inpatient or residential treatment, prescribing or detox, care planned counselling, and structured day care. Data consisting of the service user's initials, date of birth, gender and drug service accessed, are collected in order to minimise double counting. The service user is identifiable from this information. Consent will need to be sought from the service user and the following steps are advised:

- Ask for consent to collect information.
- Give reasons for use of information.
- Give reasons for sharing information.
- Reassure service users that data will be kept confidential.
- Inform service users of their right not to consent.
- Keep a record that consent was given or refused.

If a service user does not consent to their personal data being given to the NDTMS, the form should not be completed.

More information on NDTMS is available on the NTA's website at www.nta.nhs.uk.

DATs and other bodies may request monitoring information to help plan new services or ensure that a service is effectively meeting its aims and objectives. You can provide this information **without consent** provided it does not identify any individuals.

This information is usually in the form of simple, aggregated statistical data, for example:

- number of service users (50)
- age range (21-30: n=40, 31-50: n=10).

The raw data or individual records used to generate this information must be processed by the data controller who has consent to store it (i.e. the drug treatment service). It is not possible to send individual records to other parties without consent.

7.3 Can drug services use codes and not names?

Although using codes and not names may make identifying individuals more difficult, the service user can still be identified if the coding system is acquired, or by inference due to other information recorded about them. Codes may make the information slightly more secure but the personal information kept will still be covered by the rules of the Data Protection Act. Consent will need to be obtained and, if the information is sensitive, explicit consent will be needed.

7.4 Does using date of birth make the data identifiable?

Using a service user's date of birth will make the service user identifiable if names or initials are also recorded. This information should only be processed with consent. The NDTMS requires drug treatment services to record a service user's date of birth so that double counting can be avoided and an individual's treatment pathway can be tracked.

7.5 How does the Data Protection Act 1998 apply in a low threshold service?

Low threshold services, such as needle exchanges and outreach services, are still likely to need to comply with the principles of the Data Protection Act as they will probably record and process personal information on staff, volunteers and management committee members. If this were the only information processed, however, they would not be required to notify.

Whether the Data Protection Act will apply in the collection of service user information will depend on the type of service and whether the information collected is identifiable. A needle exchange will need to monitor an individual service user's return of needles, so the information obtained will need to be identifiable; data protection principles will apply and notification will be required. However, an outreach service may anonymise general demographic characteristics of service users and therefore data protection principles would not apply and notification would not be required, though it is good practice to explain any data collection to service users.

7.6 Does the Act stop personal information being shared between professional agencies?

Personal information can be shared between professional agencies with the consent of the service user. Most information a drug service would want to share about a service user will be sensitive personal information (e.g. health), so explicit consent will need to be obtained. Personal information can be shared with other professional agencies without the service user's consent when there are child protection concerns or risk of harm to self, public or staff. The drug service's confidentiality and information sharing policy should be explained to the service user at the initial assessment (see briefing number one in this series: *Confidentiality and information sharing* for more details).

7.7 What about recording or disclosing sensitive information on third parties?

Drug services should record service user's data with the understanding that a service user may request to see their personal file. Recording information about a third party, where the third party could be identified, should be avoided. Generally, service user notes should not detail names and other personal data of third parties.

If disclosure of a service user's personal information would allow the third person to be identified, a drug treatment service must obtain that person's consent before disclosure. If the third party refuses to consent then this information cannot usually be disclosed.

7.8 Can health professionals process personal information without consent?

Personal information can be processed to protect the vital interests of the data subject, in a life or death situation, such as the disclosure of a data subject's medical history to a hospital accident and emergency department treating the data subject after a serious road traffic accident.

For any further questions please contact the data protection enquiry line on 01625 545 745 or e-mail data@dataprotection.gov.uk

8 Recommended references

Data Protection Register website at www.dpr.gov.uk.

Department of Health (2000) *Data Protection Act 1998: protection and use of patient information*. London: Department of Health.

Department of Health (2000) *Data Protection Act 1998: guidance to social services*. London: Department of Health.

Department of Health (1999) *Health Service Circular 1999/053: For the record*. London: Department of Health.

HMSO (1998) *Data Protection Act 1998*. London: HMSO

Information Commissioner's website at www.dataprotection.gov.uk.

Developing drug service policies

Briefings for managers of drug treatment services

The National Treatment Agency is publishing a series of briefings to enable the managers of drug treatment services to develop effective management policies and procedures. The briefings will provide managers with:

- a summary of key policies and related issues
- guidance on implementation.

The guidance does not constitute legal advice. Individual guidance will indicate if the NTA considers it necessary to seek legal advice.

There will be ten briefings within the *Developing drug service policies* series - all of them available at www.nta.nhs.uk.

Developing drug service policies. Briefing no. 2: Data protection and record retention

Written by Julie Virgin, DrugScope.

© National Treatment Agency, London, September 2003. The text in this document may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material not being used in a derogatory manner or in a misleading context. The source of the material must be acknowledged as the National Treatment Agency and the title of the document must be included when being reproduced as part of another publication or service.



National Treatment Agency for Substance Misuse

National Treatment Agency
5th Floor, Hannibal House,
Elephant and Castle,
London SE1 6TE
Tel: 020 7972 2214
Fax: 020 7972 2248
Email: nta.enquiries@nta.nhs.uk
www.nta.nhs.uk



DrugScope
32-36 Loman Street,
London SE1 0EE
Tel: 020 7928 1211
Fax: 020 7928 1771
Email: enquiries@drugscope.org.uk
www.drugscope.org.uk