

Data Protection Policy

Version 2.11

20th May 2004

Author Susan O'Connell

Table of Contents

GLOUCESTERSHIRE PARTNERSHIP	
TABLE OF CONTENTS	2
1. INTRODUCTION	3
1.1 SCOPE	3
2. DEFINITIONS	4
2.1 DATA	4
2.2 PERSONAL DATA	5
2.3 PROCESSING	5
2.4 DATA SUBJECT	5
2.5 DATA CONTROLLER	5
2.6 DATA PROCESSOR	6
2.7 RECIPIENT	6
2.8 THIRD PARTY	6
3. PRINCIPLES	6
3.1 FIRST PRINCIPLE	6
3.2 SENSITIVE PERSONAL DATA	7
3.3 CONDITIONS FOR PROCESSING PERSONAL DATA	8
3.4 SECOND PRINCIPLE	8
3.5 THIRD PRINCIPLE	9
3.6 FOURTH PRINCIPLE	9
3.7 FIFTH PRINCIPLE	9
3.8 SIXTH PRINCIPLE	9
3.9 SEVENTH PRINCIPLE	10
3.10 EIGHTH PRINCIPLE	10
4. INDIVIDUALS RIGHTS	10
4.1 THE RIGHT TO SUBJECT ACCESS	11
4.2 THE RIGHT OF RECTIFICATION, BLOCKING, ERASURE AND DESTRUCTION	11
4.3 THE RIGHT TO PREVENT PROCESSING	11
4.4 THE RIGHT TO PREVENT PROCESSING FOR DIRECT MARKETING	11
4.5 THE RIGHT TO COMPENSATION	11
4.6 RIGHTS IN RELATION TO AUTOMATED DECISION-TAKING	11
5. RIGHT OF SUBJECT ACCESS	11
5.2 WHAT INFORMATION ARE PEOPLE ENTITLED TO?	12
5.3 REQUESTS FROM STAFF	13
5.4 EXEMPTIONS	13
5.5 SPECIAL CONDITIONS	13

<u>6. CRIMINAL OFFENCES</u>	14
<u>6.1 NOTIFICATION OFFENCES</u>	14
<u>6.2 PROCURING AND SELLING OFFENCES</u>	14
<u>6.3 ENFORCED SUBJECT ACCESS OFFENCE</u>	15
<u>6.4 OTHER OFFENCES</u>	15
<u>7. STAFF RESPONSIBILITIES</u>	15
<u>7.1 ADMINISTRATION</u>	15
<u>7.2 DEPARTMENT HEADS</u>	16
<u>7.3 CLAUSES</u>	16
<u>7.4 DOCUMENTATION</u>	16
<u>7.5 TRAINING</u>	17
<u>7.6 DATA SECURITY & CONFIDENTIALITY</u>	17
<u>7.7 POLICY REVIEW</u>	17

1. Introduction

1.1 Scope

The Data Protection Act 1998 which came into force on 1 March 2000 is about the rights and freedoms of living individuals and in particular their right to privacy in respect of personal information. The Act strengthens and extends the data protection legislation created by the Data Protection Act 1984, which has now been repealed.

Personal Data covers both facts and opinions about a living individual. It includes information regarding the intentions of the Data Controller (Gloucestershire Partnership NHS Trust) towards the individual, although in some limited circumstances exemptions will apply.

There are a number of important differences between the 1998 Act and the previous 1984 Act. The 1998 Act now includes certain data held in manual records as well as computerised data.

The main differences are:

- The Data Protection Registrar is now called the Information Commissioner.
- Data Protection Registration is now called Notification and is renewable annually.
- There are still 8 Data Protection Principles but they differ in the new Act.
- It gives individuals more rights.
- Manual records are now included.
- New processing conditions exist.
- There are now restrictions of transfer of data to non-EEA countries (European Economic Association) Includes Austria, Belgium, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, UK.

The 1998 Act stipulates those who record and use personal information must be open about how the information is used and must follow good information handling practices. It applies to the collection, use, disclosure, retention and destruction of data.

This document will describe standards for the use of personal information and guidance on individuals rights under the Data Protection Act 1998 and should be read in conjunction with:

The Information Sharing Agreement
IT Security Policy
Records Strategy
Health Records Standards
Subject Access Guidance

2. Definitions

2.1 Data

Data under the Act means information which:-

- a) Is being processed electronically. i.e. Information systems, data bases, including microfiche, audio and video systems (CCTV) and telephone logging systems.
- b) Is recorded with the intention that it shall be processed by equipment.
- c) Is recorded as part of a relevant filing system. i.e. manual files and records forming part of a relevant filing systems structured either by reference to individuals or criteria relating to individuals, rolodex, non-automated microfiches.
- d) Is an accessible record summarised as a health record, educational record, local authority housing record, or local social services record.

2.2 Personal Data

Personal data are defined in the Act as follows:

“data which relate to a living individual who can be identified”

- from those data, or
- from those data and other information which is in the possession of, or is likely to come in to the possession of the data controller (Gloucestershire Partnership NHS Trust)

2.3 Processing

The definition of processing is far wider than detailed in previous legislation. It includes:-

- Obtaining
- Recording
- Retrieval
- Consultation
- Holding
- Disclosing
- Use
- Transmission
- Erasure
- Destruction

2.4 Data Subject

Data Subject means an individual who is the subject of the personal data. A data subject must be a living individual.

2.5 Data Controller

The individual, company or organisation who determines the purpose and the manner in which personal data may be processed. The Data Controller is Gloucestershire Partnership NHS Trust.

2.6 Data Processor

Data Processor in relation to personal data, means any other person other than an employee of the Data Controller (Gloucestershire Partnership NHS Trust) who processes data on behalf of the Data Controller.

2.7 Recipient

Recipient, in relation to personal data means any person to whom data are disclosed (including employees or agents) of the Data Controller.

2.8 Third Party

Third party, means any person other than:

- the data subject
- the data controller
- any processor or other person authorised to process for the data controller

3. Principles

There are eight Data Protection Principles in the Act. Data Controllers must comply with these principles.

3.1 First Principle

“Personal data shall be processed fairly and lawfully.”

Personal data shall not be considered processed fairly unless certain conditions are met. The Data Controller 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
- 1`any other information necessary to ensure fairness: such as the likely consequences of processing, and whether they envisage the data being disclosed to a third party.

Processing may only be carried out where one of the following conditions are met:

- The individual has given his or her consent to the processing.
- The processing is necessary for the performance of a contract with the individual.
- The processing is required under legal obligation.
- The processing is necessary to protect the vital interests of the individual; or to carry out public functions.
- The processing is necessary to comply with any legal obligation to which the data controller is subject.
- The processing is necessary for the administration of justice
- The processing is necessary for Crown, Ministerial or Government functions.
- In the functions of public interest.

3.1.1 Sensitive Personal Data

The Act makes specific provision for sensitive personal data. Sensitive data includes:

- Racial or ethnic origin
- Political opinions
- Religious or other beliefs
- Trade union membership
- Physical or Mental Health
- Sexual life
- Alleged offences
- Criminal proceeding or convictions

3.1.2 Conditions for Processing Personal Data

Sensitive data can only be processed under strict conditions, which include

- Having the explicit consent of the individual
- Being required by law to process the data for employment purposes
- Needing to process the information in order to protect the vital interests of the data subject or another
- Dealing with the administration of justice or legal proceedings
- For Medical purposes
- The information has been made public by the individual
- To safeguard the rights and freedoms of the individual

3.2 Second Principle

“Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in a manner incompatible with that purpose”

The Act requires that the data controller (Gloucestershire Partnership NHS Trust) must specify the purpose of processing data (e.g. for the administration of Health Care) what data is to be included in this purpose, whom it will be disclosed to and if it is to be transferred overseas.

In doing so the Trust has to consider that data that it requires. The current purposes that the Trust has notified to the Information Commissioner are:

1. Staff Administration
2. Accounts & Records
3. Health Administration and Services
4. Research
5. Crime Prevention and Prosecution of Offenders
6. Public Health
7. Advertising Marketing and Public Relations
8. Licensing and Registration
9. Accounting & Auditing
10. Education
11. Handling and Monitoring of Complaints
12. Administration of Justice (Mental Health Act Reviews)
13. Social Services and Social Work
14. Information and Databank Administration

This register is maintained by the Information Commissioner and can be consulted by individuals to find out what processing of personal data is being carried out by a particular data controller. If the Trust does not keep its entry in the register up to date, as the data controller, it is committing an offence and can be prosecuted in the courts with a fine of up to £5000 in the Magistrates Court, or an unlimited amount in the Crown Court.

The information that is required for notification includes:

- Name and address of data controller
- Nominated representative
- Description of the personal data being processed and the category of data subject to which they relate
- Description of the purpose(s) for which the data are being processed
- Description of any recipients to whom the data will be disclosed
- Names of any countries outside the EEA to which data is or will be transferred
- Security measures to comply with Principle 7

Should any member of staff be processing personal data for any purpose other than those listed then you should immediately inform the Data Protection Manager on 01452 –89 1060.

3.3 Third Principle

“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were processed “

You should seek to identify the minimum amount of information required to fulfil the purpose. Collect only data that is required for a specific purpose. Do not request additional information unnecessarily.

3.4 Fourth Principle

“Personal data shall be accurate and where necessary, kept up to date “

You must take reasonable steps to ensure that all data is accurate. Is the fact that the data are out of date likely to cause damage or distress to the individual.

3.5 Fifth Principle

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes”

You will need to review personal data files regularly and archive the information that is no longer required.

Please refer to the Trust Records Strategy and For the record managing records in NHS Trusts and health authorities HSC 1999/053 for guidelines to retention periods for various types of data.

3.6 Sixth principle

“Personal Data shall be processed in accordance with the rights of the data subjects”

As a Data Controller we have to respond in a timely manner to subject access requests, or a request to prevent processing. (Please see section 4 for specific information)

3.7 Seventh Principle

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental damage or destruction of personal data “

You must ensure that data is kept securely. This means that the data itself is safe from corruption, deletion, change and physical damage. The Trust is obliged to offer guarantees of what security measures are in place. Please refer to the IT Security Policy.

3.8 Eighth Principle

“Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensure that an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data “

- Countries that are in the EEA - European Economic Association Include Austria, Belgium, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, UK.

4. Individuals Rights

The Data Protection Act 1998 gives individuals certain rights regarding their personal data.

4.1 The right to subject access

The Act allows individuals to find out what information is held about themselves on computer and some paper records. This is known as the right of subject access. (See section 5)

4.2 The right of rectification, blocking, erasure and destruction.

The Act allows individuals to apply to the Court to order a Data Controller to rectify, block, erase or destroy personal details if they are inaccurate or contain expressions of opinion which are based on inaccurate data.

4.3 The right to prevent processing

An individual can ask a Data Controller to stop or request not to begin process data relating to them where it is causing, or likely to cause, substantial unwarranted damage or distress to themselves or anyone else. This right is not available in all cases.

4.4 The right to prevent processing for direct marketing

A data subject can ask a data controller to stop or not to begin processing data relating to him for direct marketing purposes. This is an absolute right.

4.5 The right to compensation

A data subject can claim compensation from a data controller for damage or damage and distress caused by a breach of the Data Protection Act. Compensation for distress alone can only be claimed in limited circumstances.

4.6 Rights in relation to automated decision-taking

An individual can ask a data controller to ensure that no decision which significantly affects them is based solely on processing his or her personal data by automatic means.

5. Right of Subject Access

Any request by an individual (data subject) for access to information that you hold about them must be made in writing (this includes transmission by electronic means).

The written request must contain sufficient information to enable you to undertake the search required (e.g. Name, Address and Date of Birth). You are not obliged to comply with individuals' request until the requester has given you adequate information.

Any request for subject access to a health record should be directed to the Health Records Department at either

Health Records Department
Wotton Lawn Hospital
Horton Road
Gloucester
GL1 3WL

Health Records Department
Charlton Lane Centre
Charlton Lane
Cheltenham
GL53 9DZ

It is advisable to verify a person's identity by asking the individual to produce a copy of their driving licence or credit card. You do not have to release the information until the request has been received in writing and the required fee has been paid.

5.1 The fees that can be charged are:

Under the Data Protection Act 1998 (Fees and Miscellaneous Provisions) Regulation 2001 the fees that may be charged to view a health record or be provided with a copy are:

£10.00	Maximum fee for copies of health records held on computer only
£50.00	Maximum fee for copies of health records held manually
£50.00	Maximum fee for copies of health records held in part on computer and in part manually
£10.00	To view the record where no copies required and changes have not been made in the last 40 days
No Fee	To view the record where no copy is required and changes have been made to the record in the last 40 days

The maximum fee that can be charged is £50.00. This includes photocopying, postage and packing. The £50.00 will not be charged in all cases but on a recovery basis.

5.2 What information are people entitled to?

You must comply with an individual's request within 40 days of receipt of the written request and the fee. Once this has been received the individual is entitled to be told if any personal data are held about them and, if so:

- to be given a description of the data;
- to be told for what purposes the data are processed and

- to be told the recipients or the classes of recipients to whom the data may have been disclosed.

They are also entitled;

- to be given a copy of the information with any unintelligible terms explained;
- to be given any information available to the controller about the source of the data;
- to be given an explanation as to how any automated decisions taken about them have been made

The Information Commissioner has produced a leaflet "Your right to know" this should help explain to individuals what their rights are, these are available from the Data Protection Manager

5.3 Requests from Staff

The Trust recognises the importance of respecting the privacy of our employees and the need for appropriate safeguards in relation to the collection, storage and other processing of personnel data.

Requests from staff wanting to have access to their personal data should contact the Human Resource Department.

5.4 Exemptions

There are a number of exemptions from various provisions of the Act. 9 main exemptions are referred to as the primary exemptions, and there are 11 further miscellaneous exemptions. For further information on exemptions under the Act contact the Data Protection Manager

5.5 Special conditions

Once the request has been received you must not make any amendments or deletions to the data that would not have otherwise been made.

The data must not be tampered with in order to make it acceptable.

You do not have to comply with a request where you have already complied with an identical or similar request by the same individual, unless a reasonable interval has elapsed. In deciding what a reasonable interval is you must take into consideration the nature of the data, why the data is used and the frequency which the data is altered

**** If information is requested by a patient, and this identifies an individual as the source of the information (e.g. a relative has provided certain information), this can only be released if that individual consents to the release, or where it is seen as reasonable to comply to the request without that individuals consent (questions regarding the duty of confidence owed to the individual must be taken into consideration).**

Solicitors and insurance companies will make requests. The person involved must sign a written consent form which needs to be received before any information is released.

6. Criminal Offences

6.1 Notification offences

These are committed where processing is being undertaken by a data controller who has not notified the Commissioner either of the processing being undertaken or of any changes that have been made to that processing.

6.2 Procuring and selling offences

It is an offence to obtain, disclose, sell or advertise for sale, or bring about the disclosure of personal data, without the consent of the data controller. It is also

an offence to access personal data or to disclose it without proper authorisation

6.3 Enforced subject access offence

It is an offence for a person to ask another person to make a subject access request in order to obtain personal data about that person.

6.4 Other offences

It is an offence to fail to respond to an information notice or a breach of enforcement notice from the Commissioner.

Unauthorised disclosures by the Commissioner or his staff are forbidden and breach of those provisions or an offence.

7. Staff Responsibilities

7.1 Administration

The Trust shall ensure that it has access to specialist advice regarding the requirements of the Data Protection Act 1998. This will be provided in the first instance by the Trust's Data Protection Manager and then by the office of the Information Commissioner.

The above mentioned specialist advice will take the form of ensuring that the Trust has allocated responsibilities to a Data Protection Manager, overseen by The Information Governance Group

- Policies and procedures required by the Act.
- The Trust's registrations under that Act.
- The subject access requests.

- Staff training.
- Data Protection Issues.

7.2 Department Heads

Department Heads, Service and Line Managers must ensure that they keep a log of all their systems and manual files that process personal data. To oversee these systems they will need to nominate an Application System Manager (Please refer to the IT Security Policy Section 2.2.3) who will:

- Ensure that the systems are used within the terms of the Trust's notification and the requirements of the Data Protection Act 1998 and the Trust's policy, paying particular attention to the 8 Data Protection Principles.
- Restrict the use of the system to those authorised to do so.
- Restrict access to data on a need to know basis.
- Maintain appropriate security measures for the system and manual files in accordance with the IT Security Policy.
- Ensure that all copies of personal data are securely processed including Obtaining, recording, retrieval, consultation, holding, disclosing, use, transmission, erasure, destruction.
- Ensure that the data in the system is accurate and is kept up to date, and that the department is aware of the Department of Health guidelines on Records Management HSC 1999/053 and the Trusts Records Strategy ensuring that personal data is not kept for longer than is necessary.
- Ensure that all records may be obtained within the required 40 days of a subject access request and keep records of these access requests.
- Ensure that all users of systems and records have been properly trained on the Data Protection Act.
- Ensure that the Trust Data Protection Manager is advised immediately of any problems or complaints.

7.3 Clauses

The Trust shall, by appropriate clauses in staff contracts ensure that all staff are bound by the requirements of the Data Protection Act.

7.4 Documentation

The Trust will maintain a record of its notifications of personal data held and the purposes under the Data Protection Act. This record will be held by the Trust's Data Protection Manager.

The Trust will keep details of all subject access requests together with details of any unauthorised disclosures that have been reported by Trust staff,

together with what measures have been taken to ensure that such disclosures are not repeated.

7.5 Training

The Trust's Data Protection Manager in conjunction with the Training Department and Line Managers will ensure that all staff are aware of the Trust's policies and procedures and ensure that that staff are familiar with these.

The Trust Data Protection Manager will periodically produce and send out staff guides on Data Protection and Confidentiality.

7.6 Data Security & Confidentiality

All Trust staff will ensure that all the Trust's personal data are secured from loss, corruption, damage disclosure etc by complying with the Code of Confidentiality, IT Security Policy and Information Sharing Agreement.

7.7 Policy Review

This Policy will be reviewed annually by the Trust's Data Protection Manager and will take in to account any changes in legalisation.