

DARLINGTON PRIMARY CARE TRUST

DATA PROTECTION POLICY

Author: T W Pinnegar
Approved by: PCT Management Team

Darlington Primary Care Trust Data Protection Policy

1. Policy

It is the policy of Darlington Primary Care Trust ("the PCT") that all processing of personal data by, or on behalf of the PCT - whether as a Data Controller or as a Data Processor for others – shall be in accordance with the requirements, as currently understood, of: -

- The Data Protection Act 1998 and any subsequent amendments and Statutory Instruments which may be approved by Parliament.
- The Data Protection Registration of the PCT currently operative.
- The requirements of the PCT's Codes of Practice on the Protection and Use of Patient Information as currently operative.

Particular care is required in the handling of personal health data, whether located in automated or manual processes, and the PCT is committed to achieving the highest standards possible in this area.

2. Administration

2.1 The PCT will ensure that it has access to specialist advice regarding the requirements of the Data Protection Act 1998.

2.2 The PCT will ensure that it has allocated responsibilities for compliance to a Data Protection Co-ordinator for: -

- Overseeing the policies and procedures required by the Data Protection Act 1998 and subsequent regulations.
- Maintaining the PCT's registration under the Act.
- Carrying out compliance checks on the PCT's data usage.
- Overseeing the processing of subject access requests and ensuring that they are processed within 40 days.
- Maintaining the PCT's Data Protection and Complaints Log.
- Maintaining the PCT's Subject Access and Disclosure Log.
- Provision of information to staff on the requirements of the Data Protection Act and any amendments to it.
- Ensuring that staff who carry out special responsibilities under the Act are kept up-to-date with the developing requirements of data protection.
- Ensuring that no new systems containing personal data, or new uses of existing systems, are introduced without making appropriate changes to the PCT's registration under the Act.

- 2.3 The PCT will ensure that all systems capable of processing personal data either electronically or manually shall be supervised by a data controller who shall: -
- Ensure that the system is used within the terms of the PCT's registration and the requirements of both the Data Protection Act 1998 and the relevant Code of Practice, paying particular attention to the data protection principles as specified in the Act.
 - Restrict the use of the system to those authorised users who need access to it for PCT or other authorised work.
 - Restrict the access to particular sets of personal data available from the system to those authorised users who need access to them for PCT or other authorised work.
 - Maintain appropriate security measures for the system and any personal data held within it to avoid loss of the personal data or unauthorised disclosure of the personal data.
 - Ensure that all copies of personal data output, or obtained, from the system, whether recorded on paper, microfilm, computer readable media or any other form, are securely destroyed or erased when they are no longer required for PCT purposes.
 - Ensure that personal data held in the system are as accurate as possible and kept up-to-date where relevant and that the department has an effective policy for erasing or deleting and removing personal data as soon as they are no longer required for PCT purposes.
 - Ensure that all personal data can at all times be obtained expeditiously from the system when required to process subject access requests.
 - Ensure that all authorised users of the system containing personal data have been properly trained and advised of the PCT's requirements in respect of Data Protection.
 - Ensure that personal data are not removed from PCT premises except where specifically required for the execution of the legitimate functions of the PCT, and then only by:-
 - medical consultants or their equivalent
 - professional advisors
 - other staff with the express permission of the relevant Director.
 - Ensure that the Data Protection Co-ordinator is advised as soon as possible of any problems or complaints that should be recorded in the Data Protection and Complaints Log and of any subject access or unauthorised disclosures that should be recorded in the Subject Access and Disclosure Log.
- 2.4 The PCT shall, by appropriate clauses in their contracts or otherwise, ensure that members, staff, agents and other contractors to the PCT are bound by the requirements of the Data Protection Act, the PCT's registration and the appropriate Code of Practice.
- 2.5 Whenever the PCT functions as a Data Processor for a third party it shall only process personal data for another registered Data Controller and it shall ensure the security of the personal data entrusted to it. Disclosures of those data shall only be made with the consent of the registered Data Controller.
- 2.6 The PCT shall require suppliers of computing hardware, computing software or computing maintenance services to observe the requirements laid down by the PCT and as specified in the certification document provided to them.

3 Documentation

- 3.1 The PCT shall maintain a record of its notifications (registrations) under the Data Protection Act, which can be inspected at convenient times at the PCT's offices by staff, patients or any other interested individuals.
- 3.2 The PCT shall make available a simplified listing of its registrations for the use of its own staff and for data subjects wishing to make subject access requests.
- 3.3 The PCT shall maintain a Data Protection and Complaints Log which records significant activities and events in connection with the PCT's implementation of the Data Protection Act 1998. It will also record any complaints about these activities that may need to be recorded for inspection by the Data Protection Commissioner, or a court of law, as evidence that it has made appropriate efforts to comply with the Data Protection Principles.
- 3.4 The PCT shall maintain a Subject Access and Disclosure Log, which monitors the progress of subject access requests and records the existence of any unauthorised disclosures, together with any steps taken to ensure that such disclosures are not repeated.

4 Training

- 4.1 The PCT shall ensure that its members, staff, contractors and agents are aware of its policies and requirements regarding Data Protection and appropriate training arrangements should be made available, bearing in mind the number and turnover of staff concerned.
- 4.2 The PCT shall make available simple explanatory leaflets detailing the general responsibilities of those handling personal data. These leaflets will help to reinforce the training of such individuals. They will also advise staff on the limitations within which they should function in order to comply with the PCT's registration under the Data Protection Act, the PCT's policies in respect of Data Protection and the Code of Practice on Confidentiality.

5 Word Processing and Electronic Mail

The PCT shall ensure that its use of word processing and electronic mail systems is kept within the strict definitions of the Data Protection Act concerned with "*preparing the text of documents*". Otherwise they must be registered and fully integrated into the arrangements for administering Data Protection within the PCT.

6 Data Security and Confidentiality

- 6.1 The PCT shall ensure that its various holdings of personal data are properly secured from loss or corruption and that no unauthorised disclosures of personal data are made.
- 6.2 The PCT shall ensure that a Code of Practice on the Protection and Use of Patient Information exists in each department handling personal data, that all members of staff are aware of its existence and that they adhere to its provisions.

k:\dataprot\policy(darlington).doc