NORTH DERBYSHIRE CCG

HARTINGTON SURGERY

POLICY FOR PRIMARY CARE

DATA PROTECTION POLICY

Document History

Version Date:	September 2010
Version Number:	
Status:	Approved
Next Revision Due:	September 2012
Developed by:	Julie Coles in accordance with DCPCT policy
Policy Sponsor:	
EQIA completed:	
Approved by:	Hurst, Woods & Hurst
Date approved:	September 2010

Revision History

Version	Revision date	Summary of Changes
	01/09/12 01/09/13 01/09/14 15/01/16 28/04/17	No change Updated No change
	15/04/19	Reviewed – no change

DATA PROTECTION POLICY

Content:

DATA PROTECTION POLICY

The information and guidelines within this policy are important and apply to Hartington Surgery. This policy covers the records held and processed by staff employed by Hartington Surgery. A Code of Conduct in respect of Confidentiality will be issued under separate cover.

1 INTRODUCTION

Hartington Surgery (the Organisation) holds and processes information about its employees, patients and other individuals for various purposes (for example, the effective provision of healthcare services or to operate the payroll and to enable correspondence and communications). To comply with the Data Protection Act 1998 ("the 1998 Act") and it's principles, information must be collected and used fairly, stored safely and not disclosed to any unauthorised person. The 1998 Act applies to both manual and electronically held data.

2 SCOPE OF POLICY

This policy covers records held and processed by the organisation. The Organisation is responsible for its own records under the terms of the 1998 Act, and it has submitted a notification to the Information Commissioner – Registry No. Z6256287.

3 SUMMARY OF AIMS

The lawful and correct treatment of personal information is vital to successful operations, and to maintaining confidence within the organisation and the individuals with whom it deals. Therefore, the organisation will, through appropriate management, and strict application of criteria and controls:

- observe fully conditions regarding the fair collection and use of information;
- meet its legal obligations to specify the purposes for which information is used;
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- ensure that the rights of people about whom information is held can be fully exercised under the 1998 Act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information.);
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards.

4 NOTIFICATION TO THE INFORMATION COMMISSIONER

The Organisation has an obligation as a Data Controller to notify the Information Commissioner (formerly called the Data Protection Registrar) of the purposes for which it processes personal data. Notification monitoring within the Organisation is carried out by the Information Governance Manager. Individual data subjects can obtain full details of the Organisation's data protection registration/notification with the Information Commissioner from the Information Governance Manager or from the Information Commissioner's website (http://www.ico.gov.uk).

5 DATA PROTECTION PRINCIPLES

The Organisation, as a Data Controller, must comply with the Data Protection Principles that are set out in the 1998 Act. In summary these state that personal data shall:

- Be processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for specified and lawful purposes and shall not be processed in any manner incompatible with those purposes.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for those purposes.
- Be processed in accordance with the data subject's rights under the 1998 Act.
- Be the subject of appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that county or territory has equivalent levels of protection for personal data.

6 PROCESSING

"Processing", in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking or erasure or destruction of the information or data.
(e) viewing personal data, even where no changes are made to the data.

7 RESPONSIBILITIES OF INDIVIDUAL DATA USERS

All employees of the Organisation who record and/or process personal data in any form (called "Data Users" in this policy) must ensure that they comply with:

- the requirements of the 1998 Act (including the Data Protection Principles)
- the Organisation's Confidentiality Code of Conduct

Consideration of the principles of the 1998 Act should be made:

1. when developing a new computer system for processing personal data

2. when using an existing computer system to process personal data for a new purpose

3. when creating a new manual filing system containing personal data;

4. when using an existing manual filing system containing personal data for a new purpose.

8 ACCURACY OF DATA

All staff are responsible for:

- checking that any personal information they provide to the Organisation in connection with their employment is accurate and up to date, e.g. change of address. The Organisation cannot be held responsible for any errors unless the member of staff has informed the Organisation about them.

- checking that any patient, staff or other individual's information they handle is as accurate and up to date as possible.

9 CCTV

A number of CCTV cameras are present on the Organisation's sites. The notified purposes of the CCTV Systems are:

- Preventing and detecting crime.
- Apprehending and prosecuting offenders.
- Protecting public safety.
- To assist with security for staff, patients, other individuals and their property, in accordance with the Organisation's 'notification' to the Information Commissioner. If you have any queries regarding the operation of or access to the CCTV system, please speak to the person responsible for CCTV on the site concerned.

10 E-MAIL

It is permissible and appropriate for the Organisation to keep appropriate records of internal communications, provided such records comply with the Data Protection principles.

However, all Organisation staff need to be aware that:

- the 1998 Act applies to emails which contain personal data about individuals which are sent or received by Organisation staff;
- subject to certain exceptions, individual data subjects will be entitled to make a data subject access request and have access to emails which contain personal data concerning them, provided that the individual data subject can provide sufficient information for the Organisation to locate the personal data in the emails; and that that search would satisfy 'the temp' test as described in Durant v Financial Services Agency et at.
- the legislation applies to all emails from and to members of the Organisation which are sent and received for Organisation purposes;
- emails like other Organisation correspondence, need to be managed and archived for as long as necessary in order to meet local and corporate business needs.

11 PERSONAL DATA

Personal data is that which relates to an individual and they can be identified from that data (or from that data and other information which is in someone's possession, or may come into their possession).

12 SENSITIVE PERSONAL DATA

The Organisation may from time to time process "sensitive personal data" relating to staff, patients and other individuals.

"Sensitive personal data" relates to the racial or ethnic origin of a data subject, their political opinions, religious beliefs, trade union membership, sexual life, physical or mental health or condition or criminal offences or record.

In circumstances, where sensitive personal data are to be held or processed, the Organisation will normally seek **the explicit consent** of the individual in question, unless one of the limited exemptions provided in the Data Protection Act 1998 applies. (i.e. to perform a legal duty regarding employees, or to protect the data subject's, or a third party's vital interests).

13 DATA SECURITY AND DISCLOSURE

All staff within the Organisation are responsible for ensuring that:

- Any personal data that they hold is kept secure, relative to the security level of the data.
- Personal data are not disclosed either orally or in writing or otherwise to any unauthorised third party, and that every reasonable effort will be made to see that data is not disclosed accidentally.

Unauthorised disclosure is a disciplinary matter and may be considered gross misconduct.

Personal data must be kept secure, and examples of how this may be done will include:

- keeping the data locked in a filing cabinet, drawer or room; or
- if the data is computerised, ensuring that the data is password protected or kept only on disk which is itself kept securely; or
- any other appropriate security measure (refer to IM&T Security Policy Manual)

14 DATA SUBJECTS' CONSENT

Certain types of personal data may be processed for particular purposes without the consent of individual data subjects. However, it is the Organisation's policy to seek express consent whenever practicable from individual data subjects for the main ways in which the Organisation may hold and process personal data concerning them. This is to allow individuals an opportunity to raise any objections to any intended processing of personal data. The Organisation will consider any such objections but reserves the right to process personal data in order to carry out its functions as permitted by law.
Patient consent, should they lack capacity, this should be discussed with the next of kin or other advocate. All parties must act in the patient's interest.

15 RIGHT TO ACCESS PERSONAL DATA

Staff, patients and other individuals have the right under the 1998 Act to access (subject access request) any personal data that is being held about them either in an "automatically processable form" (mainly computer records) or in a "relevant filing system". (i.e. any set of information structured in such a way that specific information relating to a particular individual is readily accessible). They also have the right to request the correction of such data where they are incorrect.

Separate procedures are available detailing how individuals can request access to personal data.

16 NOTIFICATION OF COMPLAINTS PROCEDURE

When communicating any decision made in relation to a request under the Act's general right of access, the Practice is obliged to notify the applicant of their rights of complaint. The Practice must provide details of the complaints procedure, including how to make a complaint, and must inform the applicant of his or her right to complain to the Information Commissioner if he or she is dissatisfied with the Practice's response to a valid request for information.

17 DISCLOSURE OUTSIDE THE EEA

The Organisation may, from time to time, desire to transfer personal data to countries or territories outside of the European Economic Area in accordance with purposes made known to individual data subjects. For example, the names and contact details at the Organisation of members of staff on a website may constitute a transfer of personal data world-wide. If an individual wishes to raise an objection to this disclosure, then written notice should be given to the Organisation's Caldicott Guardian.

Other personal data, even if it would otherwise constitute fair processing, must not, unless certain exemptions apply or protective measures taken, be disclosed or transferred outside the EEA to a country or territory which does not ensure an adequate level of protection for the rights and freedoms of data subjects.

18 RETENTION OF DATA

The Organisation will hold different types of information for differing lengths of time, depending on legal and operational requirements, following which they will be destroyed. This will be done in accordance with the retention periods detailed in the Department of Health's Records Management: NHS Code of Practice.