

NHS Borders

Data Protection Policy



Document Control	
File Name:	NHS Borders Data Protection Policy V1-3.doc
Version No:	1.3
Status:	Released
Author:	Ian Merritt
Version Date:	21 February 2014
Review Date:	24 Months or as required
Copyright 2014, NHS Borders	

Authorisation Control	
Policy Owner	Chief Executive
Name: Calum Campbell	Signature
	Date

Version Control

Release	Date	Author	Comments
		Dave Arkless	Review & Update of Old Policy
Draft 1.0	16 th June 2005	Dave Arkless	1 st Draft to Caldicott Group
Draft 1.0	28 th June 2005	Dave Arkless	General Consultation (intranet)
Draft 1.0	19 th September 2005	Dave Arkless	Non Clinical Risk Management Group
Draft 1.0	30 th September 2005	Dave Arkless	Partnership
Operational	3 rd October 2005	Dave Arkless	Signed off by Chief Executive
Operational	5 th July 2006	Dave Arkless	Amended address & details, page 5
Version 1.2	26 th July 2011	Ian Merritt	Minor updates to contact details and formatting
Version 1.3	21 February 2014	Ian Merritt	Minor updates to contact details and formatting

CONTENTS

1	Introduction.....	4
2	Policy Statement	5
3	Aims of the Policy	5
4	Notification	5
5	Breach of Procedure	6
6	Nominated Officer	6
	APPENDIX A – The Eight Data Protection Principles	8
	APPENDIX B – Legal terms as used in Data Protection Act 1998	9

1 Introduction

- 1.1 NHS Borders is required to collect and use personal information about people with whom it deals in order to operate. These include past and prospective patients, employees, suppliers, clients/customers and others with whom it communicates. In addition NHS Borders may occasionally be required by law to collect and use certain types of information to comply with the statutory requirements of government departments. This personal information must be dealt with irrespective on how it is collected and used whether on paper, in a computer or recorded on other material, in accordance with the requirements of the Data Protection Act 1998 (DPA98). This Policy and supporting Procedure documents is in response to NHS Borders statutory obligation under the DPA98.
- 1.2 The supporting Procedures consists of Procedure documents each relating to specific requirements. These may be added to as new legislation is introduced. For ease of use and understanding each part is designed to be read and applied as a stand-alone policy.
 - Guidance for the Secure Handling of Personal Information
 - Records Management Policy
 - Scottish Borders Multi Agency Information Sharing Protocol
 - Access to Health data guidance notes
 - Police Requests for Personal Information

Other related Policies that should be read in conjunction are:-

- IT Security Policy
- E-mail Policy
- Internet Policy

2 Policy Statement

- 2.1 NHS Borders regards the correct use of personal information as of prime importance in successfully functioning as a health organisation. NHS Borders recognises the significance that this has in maintaining confidence between itself and those with whom it deals. It will therefore ensure that all personal information is treated fairly and lawfully. As well as enabling relevant staff to share information to function effectively, personal information has to be shared in certain circumstances with other Agencies to ensure that on going care of a patient is not compromised. A policy to ensure that the security and confidentiality of staff and patient-identifiable information is maintained at all times is therefore essential. This policy is designed to address this.

3 Aims of the Policy

- 3.1 This policy and associated procedures are intended to provide guidance and advice for staff to apply the correct handling of personal information that they come into contact with or are responsible for. For this purpose NHS Borders Data Protection Policy will comply with the DPA98. The eight DPA98 Principles are reproduced in Appendix A.
- 3.2 It is vital that those concerned with a patient's care must have ready access to the information they need to provide proper care. Patients and staff must have confidence that their personal information will be kept secure and confidential. The DPA98 places an obligation on all staff to safeguard the confidentiality of personal information. This obligation is reinforced in contracts of employment, NHS good working practices (Caldicott, CSAGS) and also by professional codes of conduct.
- 3.3 An essential requirement is the need for patients and staff to be fully informed about the uses to which information about them may be put. The prime source of this information is provided by the following leaflets:- "Confidentiality and Your Health Records – Easy Reading" and "How to See your Health Records" found on the NHS Borders internet page. "Confidentiality and Your Health Records" short leaflets (flyers) are available at GP and Dental surgeries and can also be downloaded from the Data Protection intranet page. Copies of all leaflets are available on request.

4 Notification

- 4.1 The DPA98 requires that organisations that process personal data by automatic methods must notify the Information Commissioner (IC) of their intention to conduct this activity. Borders Health Board (NHS Borders) as a Data Controller is notified with the IC annually and therefore legalises the processing of personal data by all of its employees. It should be noted that independent contractors to the Board i.e. General Practitioners, Dental Practitioners and Pharmacists as Data Controllers in their own right are out with the Boards Notification and should notify with the IC themselves.

5 Breach of Procedure

- 5.1 Any suspected concerns regarding a breach of this Policy or any of the supporting procedures should be reported to the nominated Data Protection Officer listed below.
- 5.2 Staff members are reminded that breaches of the Data Protection Act could result in a formal complaint by the data subject and/or disciplinary action being taken against the staff member by NHS Borders. In addition to this, the Information Commissioner is empowered to take independent action, both against NHS Borders and also the staff member.

6 Nominated Officer

Information Governance Lead,
NHS Borders,
NHS 1 Office,
Kelso Hospital
Inch Road,
Kelso
TD5 7JP

Telephone: 01573 227 914

E-mail: ian.merritt@borders.scot.nhs.uk

APPENDICES

APPENDIX A – The Eight Data Protection Principles

1. Personal data shall be processed **fairly** and **lawfully** and, in particular, shall not be processed unless:-
at least one of the conditions in **Schedule 2** is met, and
in the case of sensitive personal data, at least one of the conditions in **Schedule 3** is also met.
2. Personal data shall be obtained only for one or more **specified** and **lawful** purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
(Be held only for lawful purposes which are described in the register entry or have been notified to the Data Subject.)
3. Personal data shall be **adequate, relevant** and **not excessive** in relation to the purpose for which they are processed.
4. Personal data shall be **accurate** and, where necessary, **kept up to data**.
5. Personal data processed for any purpose or purposes shall **not be kept for longer than is necessary** for that purpose or those purposes.
6. Personal data shall be processed in accordance with **the rights of data subjects** under this Act
7. Appropriate **technical and organisational** measures shall be taken against unauthorized or unlawful processing of personal data and against loss or destruction of, or damage to, personal data.
8. Personal data shall **not be transferred** to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

APPENDIX B – Legal terms as used in Data Protection Act 1998

(With a brief non-legal interpretation)

Data is information which -

- a) Is being processed by means of equipment operating automatically in response to instructions given for that purpose
- b) Is recorded with the intention that it should be processed by means of such equipment
- c) Is recorded as part of a relevant filing system or that it should form part of a relevant filing system or
- d) Does not fall within para a) b) or c) but forms part of an accessible record as defined by Section 68
- e) Is recorded information held by a public authority and does not fall within any of the paragraphs (a) to (d)

(facts from which information may be drawn)

Personal data

Data which relate to a living individual who can be identified-

- a) From those data, or
- b) From those data and other information which is in the possession of or is likely to come into the possession of the Data Controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

(personal data is any data relating to a living, identifiable individual)

Relevant Filing System

Any 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 criteria relating to individuals, in such a way that specific information relating to a particular individual is readily available.

(manual data that is structured by a minimum of two levels)

Recipient

Any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom the disclosure is or may be made as a result of or with a view to a particular enquiry by or on behalf of that person made in the exercise of any power conferred by law.

(any person receiving data except from those requests made by the power of law)

Third Party

Any person other than the data subject, the data controller or any data processor or other person authorised to process data for the controller or processor.

(a person out with the control of the data controller)

Data Subject

An individual who is the subject of personal data

(any living person who is the subject of personal data)

Data Controller

A person who (either jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed.

(can be a person or an organisation)

Data Processor

Any person other than an employee of the data controller who processes data on behalf of the data controller.

(such as another company, agency or health board)

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, erasure or destruction of the information or data.”

(anything done to data during its life cycle while in the control of the Data Controller, is processing)

Consent (Is not defined by the Act, however can be interpreted as follows)

Should be - Freely Given, Specific, Informed, Unambiguous

Consent may be expressed or inferred from some relevant action (implied consent) but cannot be inferred from silence.

“No one can consent to something of which he has no knowledge”

Consent in the Criminal Law