NHS
North Yorkshire and York

Title:	**DATA PROTECTION POLICY**
Reference No:	NHSNYYIG - 008
Owner:	Director of Standards
Author:	Information Governance Manager
First Issued On:	May 2009
Latest Issue Date:	February 2012
Operational Date:	February 2012
Review Date:	April 2013
Consultation Process:	Key internal stakeholders (management & staff-side); JNCC; LNC
Policy Sponsor:	Information Governance Steering Group
Ratified and Approved by:	Governance Committee
Distribution:	All staff
Compliance:	Mandatory for all permanent & temporary employees, contractors & sub-contractors of NHS North Yorkshire and York
Equality & Diversity Statement:	Compliant

CHANGE RECORD			
DATE	**AUTHOR**	**NATURE OF CHANGE**	**VERS No**
16/01/2009	IG Manager	Draft of new Policy	0.01
16/02/2009	IG Manager	Rework after initial reviews	0.02
10/05/2009	IG Manager	Rework prior to IGSG	0.03
28/05/2009	Governance Committee	Policy Approval	1.00
Sept 2010	IG Team	Review	1.01
Dec 2011	IG Team	Amended to reflect the new organisation	2.00

Preface

This Policy is made between NHS North Yorkshire and York and the recognised staff side organisations, using the mechanism of the Joint Negotiation and Consultative Committee (JNCC). It will remain in force until superseded by a replacement Policy, or until terminated by either management or staff side, giving no less than six months notice. The purpose of the notice to terminate the Policy is to provide the opportunity for both parties to renegotiate a replacement Policy. Withdrawal by one party, giving no less than six months notice, will not of itself invalidate the agreement. If agreement cannot be reached on a revised policy, then either party may refer the matter to the Advisory, Conciliation and Arbitration Service (ACAS) for conciliation.

Document Objectives

This policy sets out the approach taken within NHS North Yorkshire and York to provide a robust Data Protection framework for the current and future protection of information.

Intended Recipients

All staff.

1 Introduction

1.1 The NHS North Yorkshire and York has a legal obligation to comply with all appropriate legislation and guidance issued by professional bodies in respect of Data, Information and IT Security.

1.2 This Policy outlines how NHS North Yorkshire and York will meet its legal obligations and NHS requirements concerning confidentiality and information security standards.

1.3 The Policy relates to roles that are reliant on computer systems or manual records such as: patient administration, purchasing, invoicing and treatment planning and the use of manual records relating to patients, staff and others whose information may be held within NHS North Yorkshire and York.

2 Overview of the Data Protection Act 1998

2.1 NHS North Yorkshire and York has a duty under the Data Protection Act to hold, obtain, record, use, and store all personally identifiable information in a secure and confidential manner. This applies to all personal identifiable information held in manual files, computer databases, videos and other automated media about living individuals, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, x-rays etc.

2.2 The Act dictates that information should only be disclosed on a need to know basis. Printouts and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty.

2.3 NHS North Yorkshire and York are required to register its data holdings with the Information Commissioner, identifying the purposes for holding the data, how it is used and to whom it may be disclosed.

2.4 All applications/databases should be registered under NHS North Yorkshire and York 's global registration with the Information Commissioner and comply with the Data Protection Act 1998. This will primarily be achieved by adhering to the policies of NHS North Yorkshire and York and following the Eight Data Protection Principles listed in Annex A.

2.5 Under a provision of the Data Protection Act an individual can request access to their information, regardless of the media this information may be in.

3 Roles and Responsibilities

3.1 **Chief Executive.** The Chief Executive has overall responsibility for Data Protection within NHS North Yorkshire and York. As accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. NHS North Yorkshire and York has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

3.2 **Caldicott Guardian.** NHS North Yorkshire and York's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They will oversee disclosures of patient information with particular attention being paid to extraordinary disclosures (those which are not routine) in accordance with the NHS Confidentiality Code of Practice (November 2003).

3.3 **Director of Standards.** NHS North Yorkshire and York's Director of Standards has delegated responsibility for accountability of Data Protection under Information Governance.

3.4 **Information Governance Steering Group / Information Governance Manager.** NHS North Yorkshire and York's Information Governance Steering Group and Information Governance Manager are responsible for ensuring that this policy is implemented, through the Information Governance Strategy, and that Data Protection systems and processes are developed, co-ordinated and monitored.

3.5 **Managers / Local Team Leaders / Supervisors.** Managers, Local Team Leaders and Supervisors will ensure that all staff are:

3.5.1 Aware of the Data Protection Policy and updates in regard to any changes in the Policy

3.5.2 Attend appropriate training.

3.5.3 Have access to all systems and procedures to support the Policy.

3.5.4 Know how to deal with requests for personal/patient identifiable information.

3.5.5 Know how to access and store personal/patient identifiable information, both manual and electronic records.

3.5.6 Register databases with the Information Governance Manager who will maintain a log of databases and nominated application/system managers.

3.5.7 To notify the Information Governance Manager prior to the agreement of any contracts or agreements where information will be processed outside of the European Economic Area to facilitate a review of the information processing to ensure compliance with the Data Protection Acts eighth principle.

3.6 **All Staff.** All NHS North Yorkshire and York staff, whether clinical or administrative, who create, receive and use records have Data Protection responsibilities. All staff will be expected to:

3.6.1 Adhere to this Policy and all related systems and processes to implement the Act.

3.6.2 To attend training as appropriate.

3.6.3 To ensure that all patient/personal identifiable information is accurate, relevant, up-to-date and used appropriately, both electronic and manual including the use of databases.

3.6.4 To ensure that all patient/personal identifiable information is kept secure at all times.

3.7 **Contractors and Support Organisations.** All NHS North Yorkshire and York Contractors and Support Organisations should ensure that Service Level Agreements and contracts must include responsibilities for information governance and Data Protection as appropriate.

4 Obtaining Consent

4.1 NHS North Yorkshire and York will ensure that the general public, staff, including volunteers, locums, temporary employees and patients are aware of why the NHS needs information about them, how this is used and to whom it may be disclosed by the use of leaflets, posters and the NHS North Yorkshire and York web site. Statements about Data Protection will be included on all forms requesting personal identifiable information.

5 Databases

5.1 A database is any collection of personal information that can be processed by automated means. A few examples are detailed below:

- Patient/personal records (names and addresses etc.) for appointments
- Patient/personal information used for research e.g. where only NHS number (or other personal identifier may be allocated) and clinical details may be held -this could be an Excel spreadsheet
- Patient/personal details used for prescribing drugs

- Staff records held on Excel to monitor annual leave and sickness Information collected from individuals should be complete and should all be justified as being required for the purpose they are being requested.

6. Third Party Contracts

6.1 The Data Protection Act 1998 places a responsibility on those who are data controllers of personal data to ensure that when data processing is carried out on their behalf that they choose a processor providing specific guarantees in respect of technical and organisational security measures governing the processing to be carried out and take reasonable steps to ensure compliance with those measures.

6.2 Any data processing must be carried out under a contract evidenced in writing, under which the data processor is to act only on instructions form the data controller.

6.3 Where an organisation has assessed itself as meeting the IG assurance requirements to an appropriate level, and has recorded its assessment within the IG Toolkit, this provides a clear and structured basis for auditing the organisation to obtain assurance that IG standards are being met.

6.4 A self-assessed IG Toolkit submission does not itself provide this assurance and bodies contracting, or otherwise engaging, with organisations who have gone through the IG assurance process must ensure themselves that there is robust evidence of performance.

6.5 It is the responsibility of all NHS Contracting Authorities to ensure that appropriate IG assurance is obtained when contracting for the delivery of information services. The PCT should as a minimum ensure that those it contracts with have completed an IG Toolkit submission and have met at least Level 2 on all required criterion, and or have obtained appropriate certification against ISO27001. In some circumstances with the support of the Information Team approval for other IG assurances can be submitted to IGSG for approval.

6.6 The Information Governance Team will provide clauses for contracts that have been approved by Legal Services for the inclusion in contracts. Senior Managers, Information Asset Owners, and all PCT Managers must ensure the inclusion of such clauses in any contract they enter into, where the standard clauses are not felt to be appropriate guidance must be sought from the Information Governance Team.

6.7 To notify the Information Governance Manager prior to the agreement of any contracts or agreements where information will be processed outside of the European Economic Area to facilitate a review of the information processing to ensure compliance with the Data Protection Acts eighth principle

7 Retention of Information

7.1 All records should be retained and disposed of according to the NHS North Yorkshire and York's Records Management Policy. If in doubt contact the Information Governance Team.

8 Access to Information

8.1 NHS North Yorkshire and York will ensure that systems and processes are in place to allow staff, patients, relatives and the public to access their personal information that is held by NHS North Yorkshire and York, in accordance with the Data Protection Act 1998 and the Access to Health Records Act (deceased patients only). NHS North Yorkshire and York has a separate Staff Guidance on Access to Health Records which is available on the NHS North Yorkshire and York Intranet or through the Information Governance Team.

9 Complaints

9.1 NHS North Yorkshire and York will implement the use of the complaints procedure to deal with complaints in connection with the Data Protection Act. If the complainant is dissatisfied with the conduct of NHS North Yorkshire and York, then they can be referred to the Information Commissioner.

10 Training/Awareness

10.1 Training

10.1.1 The Information Governance Manager will work with the NHS North Yorkshire and York Training Team to ensure that training on the Act is available to all staff.

10.1.2 All clinicians and others responsible for the care of patients, and all staff responsible for writing and/or handling health records should ensure that they are aware of the terms of the Act by completing the e-learning training on Data Protection, Confidentiality and the role of the Caldicott Guardian. Further information on this training can be obtained from the Information Governance Manager or on the NHS North Yorkshire and York Intranet.

10.2 Contracts of employment

Staff Contracts of employment are produced and monitored by Human Resources Department. All contracts of employment include a data protection and general confidentiality clause. Agency and contract staff are subject to the same rules.

10.3 Awareness

NHS North Yorkshire and York will keep guidelines for staff and patients on the use of patient/personal identifiable information up-to-date and accessible to all.

11 Monitoring & Audit

11.1 This Policy and associated appendices and procedures will be monitored by the Information Governance Steering Group and it is assumed that both Internal and External Audits will review this and associated policies and procedures.

12 Information Sharing

12.1 There are Acts of Parliament that govern the disclosure/sharing of personal patient information - some make it a legal requirement to disclose and others that state information cannot be disclosed. NHS North Yorkshire and York has Information Sharing Protocols with our partners and external agencies.

13 Data Security and Confidentiality

13.1 NHS North Yorkshire and York will 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. Further details can be found in the NHS North Yorkshire and York Information Security Policy.

13.2 NHS North Yorkshire and York shall ensure that all members of staff are aware of the existence of the NHS North Yorkshire and York's Code of Conduct for Employees in Respect of Confidentiality, and that they adhere to its provisions.

13.3 NHS North Yorkshire and York will ensure that information is not transferred to countries outside of the European Economic Community (EEA) unless that country has an adequate level of protection for security and confidentiality of information and this has been confirmed by the Information Commissioner. Information on countries with an adequate level of protection and the US Safe Harbor agreements is detailed on the Information Commissioner's website at:

http://www.ico.gov.uk/what_we_cover/data_protection/international/international_transfers.aspx

14 Policy Review & Retention

14.1 This policy will be reviewed every twelve months (or sooner if new legislation, codes of practice or national standards are to be introduced).

14.2 This policy will be retained in line with the Records Management: NHS Code of Practice (Department of Health, 2009) retention schedules.

15 Equality & Diversity Statement

15.1 NHS North Yorkshire and York recognises the diversity of the local community and those in its employ. Our aim is therefore to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. NHS North Yorkshire and York

recognises that equality impacts on all aspects of its day to day operations and has produced an Equality and Human Rights Strategy and Equal Opportunities Policy to reflect this. All strategies, policies and procedures are assessed in accordance with the Equality & Diversity Assessment Toolkit, the results for which are monitored centrally.

16 Disciplinary Statement

16.1 Breaches of this policy will be investigated and may result in the matter being treated as a disciplinary offence under the NHS North Yorkshire and York's disciplinary procedure.

Annex A

THE EIGHT DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
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 unauthorised or unlawful processing of personal data and against accidental 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