NHS
North Yorkshire and York

Title:	**Pseudonymisation and Anonymisation Policy**
Reference No:	NHSNYYIG -017
Owner:	Director of Standards
Author:	Information Governance Manager
First Issued On:	March 2012 (Version1.00)
Latest Issue Date:	March 2012 (Version1.00)
Operational Date:	March 2012 (Version1.00)
Review Date:	April 2013
Consultation Process:	Key internal stakeholders (management & staff-side); Business Intelligence; Contracting
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**	**VERSION NO**
01 Feb 2012	IG Team	Draft of new Policy	0.01
13 March 2012	Governance and Quality Committee	Approval	1.00

Preface

Document Objectives

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

Intended Recipients

All staff.

Contents

1 Introduction

1.1 The aim of this policy is to enable NHS North Yorkshire and York staff to access and carry out secondary use of patient data in a legal, safe and secure manner. It is a legal requirement that when patient data is used for purposes other than direct care, i.e. Secondary Uses, the patient should not be identifiable unless otherwise legally required such as having obtained the patient's consent or Section 251 approval. This is set out clearly in the Department of Health's document 'Confidentiality: the NHS Code of Practice', which states the need to 'effectively anonymise' patient data prior to the non-direct care usage being made of the data.

The Data Protection Act 1998, the Human Rights Act 1998 and the common law relating to confidentiality apply to all organisations. They require that the minimum personal data are used to facilitate any particular purpose and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned unless there is a lawful exemption under the Data Protection or Human Rights Acts to do so. All NHS organisations must respect people's private lives. Pseudonymisation and Anonymisation is a method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item. This allows patient linking analysis needed within secondary uses. Pseudonymisation is a core element of Secondary Uses Services (SUS) and should be applied across NHS North Yorkshire and York.

1.2 NHS North Yorkshire and York has a legal obligation to comply with all appropriate legislation and guidance issued by professional bodies in respect of pseudonymisation and anonymisation.

1.3 This Policy outlines how NHS North Yorkshire and York will meet its legal obligations and NHS requirements concerning pseudonymisation and anonymisation.

1.4 The Policy relates to roles that are reliant on computer systems and 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 Purpose and Scope

2.1 This policy applies to all NHS North Yorkshire and York staff (including substantive, temporary, student, honorary staff etc) and staff working with the registered population (Commissioning Support Services and Clinical Commissioning Groups, etc), who use patient data for secondary use purposes and uses other than direct patient healthcare with guidance to safeguard the confidentiality of the patient. The policy has been developed in line with the Connecting for Health and the NHS North Yorkshire and York Pseudonymisation and Anonymisation Project.

2.2 The key principle is to ensure, as far as is practicable, that individual service users cannot be identified from data that are used to support purposes other than their direct care or to quality assure the care provided. Where this is not practicable data should flow through business processes that minimise the risk to data. In many circumstances this requires data to be received by NHS NYY staff as designated to do so under 'New Safe Haven' authorisation where it can be processed securely and only used in an identifiable form for specific authorised procedures within the New Safe Haven boundary. Onward disclosure should be limited to pseudonymised or anonymised data.

2.3 Planning guidance published by the Department of Health in support of the 2010/11 Operating Framework sets out clear targets for NHS bodies.

It states that: ***"It is NHS policy and a legal requirement that patient level data should not contain identifiers when they are used for purposes other than the direct care of patients, including local flows between organisations as well as data extracted from the Secondary Uses Service.***

NHS Commissioners should ensure that organisations from which care is commissioned comply. SHAs should ensure that organisations within their health economies comply."

2.4 This policy is in line with the Connecting for Health Pseudonymisation Implementation Project requirements.

3 Definitions

The definitions used in this policy are adopted from the Connecting for Health Pseudonymisation Implementation Project (PIP) Reference Paper 1, Guidance on Terminology.
http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo/ref1term.pdf

3.1 Patient/Personal Identifiable Data (PID)

Patient Identifiable Data is information about a person that would enable the person's identity to be established. This might be fairly explicit such as initials and surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent.

Any of these items can be considered collectively or in isolation as patient identifiable information: Surname, Forename, Initials, Address, Date of Birth, Other dates (e.g. death, diagnosis), Postcode, Gender, Occupation, Ethnic group, NHS or Hospital Number, National Insurance Number, Telephone number and Local Identifier.

3.2 Primary use

Use of data that directly contributes to the safe care and treatment of a patient and include diagnosis, referral and treatment processes together with relevant supporting administrative processes, such as clinical letters and patient administration, patient management on a ward or GP surgery, managing appointments for care; as well as the audit/assurance of the quality of the healthcare provided is considered primary use.

3.3 Secondary use

Other uses of the data, that is the non-direct care usage referred to above, are usually known as secondary uses. Examples of secondary uses are for preventative medicine, trend analysis, medical research, financial audit and the management of health care services, as set out in Confidentiality: the NHS Code of Practice, Ref 6.

3.4 Information Processing

Means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

3.4.1 Organisation, adaptation or alteration of the information or data,
3.4.2 Retrieval, consultation or use of the information or data,
3.4.3 Disclosure of the information or data by transmission, dissemination or otherwise making available, or
3.4.4 Alignment, combination, blocking, erasure or destruction of the information or data;

3.5 Caldicott Principles

The Caldicott report relates to the use of patient-identifiable information within the NHS and highlights two key points: All NHS organisations must appoint a Caldicott Guardian, and details of six key principles to be applied when using patient–identifiable information.

Compliance with these principles reduces the risk of breach of confidentiality and breaches of legal requirements. This is best practice in accordance with the NHS Confidentiality Code of Practice (November 2003) and should therefore be adopted when implementing Pseudonymisation and Anonymisation Project.

4 Roles and Responsibilities

4.1 Chief Executive

The Chief Executive has overall responsibility for Information Governance within NHS North Yorkshire and York and has a corporate responsibility for ensuring that it corporately meets its legal responsibilities. The Chief Executive also has a responsibility for the adoption of internal and external governance requirements which oversees the implementation of the pseudonymisation and anonymisation project as per the NHS Policy.

4.2 Caldicott Guardian

NHS North Yorkshire and York's Caldicott Guardian has a responsibility for review and authorisation of all procedures that relate to the use of patient identifiable information under the pseudonymisation and anonymisation project.

4.3 Director of Standards

NHS North Yorkshire and York's Director of Standards has delegated responsibility and accountability for the pseudonymisation and anonymisation project under information governance

4.4 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 New Safe Haven processes and procedures are developed, co-ordinated and monitored to comply with the NHS Operating Framework 2010/2011 for the pseudonymisation and anonymisation project.

4.5 Managers / Local Team Leaders / Supervisors

4.5.1 Identify all areas that need to be classified under this policy.

4.5.2 Nominate a member of staff to manage that classified area.

4.5.3 Identify staff that have a justified purpose to access patient-identifiable information, and obtain authorisation to access patient identifiable information from the Caldicott Guardian via the 'Caldicott Authorisation to Access patient-identifiable information for secondary uses form' implement a regular review of the appropriateness of this access. See Annex B. This level of access will be know as New Safe Haven Access.

4.5.4 Ensure all staff have completed both the Information Governance Statutory and Mandatory training and other relevant Connecting form Health Information Governance Training modules.

4.5.5 Organise the removal of staff rights to patient-identifiable information where access is no longer justified.

4.5.6 Maintain a comprehensive register of those staff authorised to access patient-identifiable information, including details of where access has been reviewed and removed, e.g. on change of duties or cessation of employment.

4.5.7 Ensure all systems holding patient –identifiable information are accessible via robust log-on and password mechanisms only and that these are allocated on a need to know basis only in line access authorised via the Caldicott Authorisation to Access patient-identifiable information for secondary uses form.

4.5.8 All managers are responsible for ensuring that this policy and its supporting standards and guidelines are successfully implemented into local processes and that there is ongoing compliance on a day to day basis. Any breaches or suspected breaches of confidentiality or information security must be reported for immediate investigation.

4.5.9 Have access to all systems and procedures to support this policy and attend appropriate training on how to deal with requests for personal/patient identifiable information and to access and store personal/patient identifiable information, both manual and electronic records.

4.6 All Staff

All NHS North Yorkshire and York staff, whether clinical or administrative, who create, receive and use patient records have pseudonymisation and anonymisation responsibilities under Data Protection Act & Information Governance requirements. All staff will be responsible for:

4.6.1 Ensuring they understand the requirements of this policy and its supporting standards and guidelines.

4.6.2 Ensuring that this policy and its supporting standards and guidelines are built into local processes and that there is ongoing compliance on a day to day basis.

4.6.3 Ensure all breaches or suspected breaches of confidentiality or information security are reported for immediate investigation.

4.6.4 Highlight areas of potential weakness to their Managers/nominated Safe Haven Managers immediately for appropriate corrective action.

4.7 Contractors and Support Organisations

All NHS North Yorkshire and York must ensure that all contracts and service level agreements with Contractors and Support Organisations include responsibilities for pseudonymisation and anonymisation under information governance and data protection requirements.

5. New Safe Havens

The NHS has used safe havens for over 20 years to ensure the secure transfer of Patient Identifiable Data (PID). The NHS North Yorkshire & York Safe Haven Policy provides the guidance related to the security of transferring/sharing information via staff delivery, fax, post, email and telephone. These requirements are detailed within the NHS North Yorkshire and York Safe Haven Policy.

The New Safe Haven principles include the concept of restricting access to patient identifiable data which is required to support the pseudonymisation process of de-identifying records. The approach to New Safe Havens is specified in the Connecting for Health Pseudonymisation Implementation Project (PIP), Reference Paper 2, Guidance on Business Processes and Safe Havens.

http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo/ref2busprosh.pdf

Patient information systems and databases must be within an electronic safe haven whereby access is limited and password controlled for each authorised user. Access to a new safe haven will be controlled via a Caldicott Authorisation to Access PID for Secondary Uses Form**.** The nomination for a member of staff to access patient identifiable data under new safe haven arrangements must be signed off by an appropriate senior manager and then submitted to the Caldicott Guardian for approval.

A register of the staff able to access patient-identifiable information must be maintained and regularly reviewed by the Information Asset Owner and available for audit by the Information Governance Team.

6. Business Process

All business processes within NHS North Yorkshire & York must be documented. Connecting for Health pseudonymisation implementation project (PIP), Reference Paper 2, Guidance on Business Processes and Safe Havens will be adopted to implement this function.

http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo/ref2busprosh.pdf

Business processes can include, but are not exclusively limited to:

6.1 Those processes using patient data involved in the direct care of patients; (Primary Use)

6.2 Those processes using patient data not involved in the direct care of patients; (Secondary use)

6.3 Combination of Primary & Secondary uses; where one of the purposes of use of patient data may be to support the direct care of patients, such as an intervention by clinicians using non direct data to identify individual patients.

The business process for primary use includes, but is not restricted to; recording care provided, appointment bookings, management of waiting lists, inputting test results and any other function that is related to administration of direct patient care.

All information recorded about a patient should be recorded in line with the Data Protection Act 1998 and the NHS North Yorkshire & York Records Management Policy.

Secondary use business processes must be undertaken with de-identified data. Any processes that are using PID must be modified in line with this policy. If the business process requires confirmation that the patient is registered within a GP practice within the NHS North Yorkshire & York area this is to be undertaken through the New Safe Haven processes.

All business processes must be regularly reviewed to monitor the impact and risks of de-identifying the data. New Safe Haven information flows and processes must be monitored if a piece of PID is a required for analysis purposes, for example postcode may be required if a geographical outcome is to be achieved.

7. De-Identification

Staff should only have access to those data that are necessary for the completion of the business activity which they are involved in. This is reflected in Caldicott Principles; ***Access should be on a need to know basis***. This principle applies to the use of PID for secondary or non-direct care purposes.

By de-identification users are able to make use of non identifiable patient data for a range of secondary purposes without having to access the identifiable data items. Connecting for Health Pseudonymisation Implementation Project (PIP), Reference Paper 3 on Guidance on De-identification will be adopted in implementing this function.

http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo/ref3deident.pdf

The aim of de-identification is to obscure the patient identifying information items within the patients record sufficiently that the risk of potential identification of the respective service user is minimised to acceptable levels, this will provide effective anonymisation. The use of multiple pseudonyms should be adopted, a single pseudonym for use within NHS North Yorkshire & York and separate pseudonym for use outside of the organisation.

When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual patients across different data sets. This allows the linking of data sets and other information which is not available if the patient identifiable data is removed completely.

Where patient identifiable data is required the NHS Number must be used as part of this data set. The NHS Number should be included within all patient records and documentation in line with the current Connecting for Health NHS Number Campaign.

8. Pseudonymisation

To effectively pseudonymise data the following actions must be taken:

8.1 An algorithm must be applied to the agreed field within the patient record, i.e. the NHS Number to generate a pseudonymised identification number, to be used on reports for secondary use purposes.

8.2 Each field of PID must have a unique pseudonym.

8.3 Pseudonyms to be used in place of NHS Numbers and other fields that are to be used by staff must be of the same length and formatted on output to ensure readability.

For example, in order to replace NHS Numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e. 5L7 TWX 619Z. Letters should be used within the pseudonym for an NHS number to avoid confusion with original NHS numbers.

8.4 Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports.

8.5 Pseudonyms for external use must be independently generated to give different pseudonym from the one used internally in order that internal pseudonyms are not compromised.

8.6 The secondary use output must only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines.

8.7 Pseudonymised data should have the same security as PID.

8.8 Further wider referencing is available via the following two documents;

Connecting for Health Pseudonymisation Implementation Project (PIP), Reference Paper 4 on Pseudonymisation Technical White Paper - Design and MS-SQL

http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo/pipwhitepaper.pdf

Connecting for Health Pseudonymisation Implementation Project (PIP), Reference Paper 4 Supplement on Pseudonymisation MS-SQL Examples

http://www.connectingforhealth.nhs.uk/systemsandservices/pseudo/whitepapercode.doc

9. Use of Patient Identifiable Information

Patient Identifiable information must only be used for justified purposes, ***on a need to know basis*** and only by those who have been authorised to do so, via the Caldicott Authorisation to Access patient-identifiable information for secondary uses form. (Annex B)

10. Information Governance Requirements

Appropriate information governance arrangements must be put in place to ensure the proper use of information and maintain the security and confidentiality of information at all times.

11. Transferring Information

Where it has been identified that information sharing is to take place with other organisations, information sharing agreements should be documented, agreed and signed up to by the Caldicott Guardians/ SIRO's of the partner organisations to that agreement.

12. Training

All staff are required to complete the statutory and mandatory information governance training on an annual basis.

Staff will be made aware of this policy and its operational requirements through line management

The policy will be available to staff via the Intranet.

13 Equality and Diversity

NHS North Yorkshire and York recognise 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. All policies and procedures are assessed in accordance with the Equality & Diversity Assessment Toolkit, the results for which are monitored centrally.

14 Review

This policy will be reviewed annually. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

15. Monitoring

15.1 Breaches in Information Governance will be reported via the NHS North Yorkshire and York's incident reporting mechanisms and will be subject to investigation.

15.2 The Information Governance Steering Group will develop a routine audit programme to monitor the adequacy of systems and policies and provide reports to the Governance Committee.

16. Discipline

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

17. Related Guidelines & References

The Caldicott Principles (Annex A)
Data Protection Act 1998
Confidentiality: The NHS Code of Practice
Common Law - Duty of Confidentiality
NHS Operating Framework 2010/11
Information Governance Toolkit, Requirement 9-324
NHS NYY Safe Haven Policy

Annex A

THE SIX CALDICOTT PRINCIPLES

Principle 1:

Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, continuing uses must be regularly reviewed by an appropriate guardian.

Principle 2:

Do not use patient identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be used unless there is no alternative.

Principle 3:

Use the minimum necessary patient-identifiable information

Where use of patient-identifiable information is considered to be essential, each individual item of information in a data set should be justified with the aim of minimising the possibility of identifying the data subject.

Principle 4:

Access to patient identifiable information should be on a strict need to know basis

Only those individuals who need access to patient identifiable information should have access to it, and this should be limited to the information items that they need to in order to undertake their duties only.

Principle 5:

Everyone should be aware of their responsibilities

Action should be taken to ensure that all staff handling patient identifiable information, whether clinical or non-clinical, are aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6:

Understand and comply with the law

Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements and all staff should be aware of their responsibility to keep patient-identifiable information secure and confidential.

Annex B

CALDICOTT AUTHORISATION TO ACCESS PATIENT IDENTIFIABLE INFORMATION FOR SECONDARY USES FORM

This Form is to be completed by the relevant Service Manager when it is necessary for a member of staff to access patient identifiable data (PID) for secondary use purposes. This form should be sent to the Caldicott Guardian for authorisation and risk assessment.

Details of User Requesting Access to PID for Secondary Use Purposes

Name		Contact Number	
Email Address			
Directorate		Department	

Details of Data to be accessed for Secondary Use Purposes

Data Description	
Types of Data User will be accessing	□ Name □ Address □ Date of Birth □ Gender □ Ethnicity □ Medical Details □ Other (please specify below)
Reason of Accessing PID	
Format of Data Transfer (i.e. electronic/paper based)	
Frequency of Data Access	□ One-Off □ Weekly □ Monthly □ Quarterly □ Annually □ Other (please sepcify below)
Proposed mechanisms to secure the data being accessed	
If applicable, what systems are used to access the PID for Secondary Use Purposes?	

Service Manager Details

Service Manager Name			
Contact Number			
Email Address			
Directorate		Department	
Service Manager Signature		Date	

CALDICOTT GUARDIAN USE ONLY

Caldicott Guardian Approval:	□ Yes □ No
If No, any reason/s	
Name (Print)	
Position	
Signature	
Date	