NHS
Cornwall and
Isles of Scilly

Pseudonymisation policy

Date approved: 16 February 2023

NHS Cornwall and Isles of Scilly Integrated Care Board

Call us on 01726 627 800
Email us at ciosicb.contactus@nhs.net
Visit our website: cios.icb.nhs.uk

Part 2S, Chy Trevail,
Beacon Technology Park,
Dunmere Road,
Bodmin, PL31 2FR
Chair: John Govett
Chief executive officer: Kate Shields

Document control

Title of document: Pseudonymisation policy
Lead directorate: Strategy, planning and corporate services
Lead team: Information governance
Document type: Policy
Subject category: Information governance
Author(s) name: Beverley Gallagher and Trudy Corsellis
Date ratified: 16 February 2023
Ratified by: Director for strategy, planning and corporate affairs
Review frequency: 3 years (standard, unless otherwise indicated)
To be reviewed by date: 16 February 2026
Target audience: All staff
Can this policy be released under FOI? Yes
Give reasons for exemption if no: N/A

Version control

Version number	Revision date	Revision by	Nature of revisions
1.1	December 2018	Deputy head of corporate governance	Updated for DPA (2018) and GDPR.
2.0	January 2023	Head of information governance	Review and update
2.1	February 2023	Carolyn Andrews, director for strategy, planning and corporate affairs	Updated policy ratified by relevant executive director

You can request any document published on our website in alternative formats. Email our engagement team for more information.

Contents

1. Introduction 5
2. Purpose 5
3. Definitions 5
Pseudonymisation and/or pseudonymised data 5
Anonymised Data 5
Primary use 6
Secondary use purposes 6
Personal confidential data (PCD) 6
Confidential patient identifiable data 6
Non-confidential patient data – Pseudonymised 7
Non-confidential patient data - Part-anonymised 7
Non-confidential patient data - Fully anonymised 7
4. Responsibilities 7
Chief executive 7
Senior information risk owner (SIRO) 7
Caldicott guardian 7
Head of information governance 8
Managers 8
Staff 8
5. General principles 8
Pseudonymisation 9
6. Pseudonymisation controls 10
7. DSCRO 10
8. Section 251 approval 11
9. Safe havens 11
10. Accredited safe havens 11
11. Controlled environment for finance 11
12. Training requirements 12
13. Implementation plans and monitoring effectiveness 12
14. Update and review 12
15. References, policies and legal framework 12
16. Consultation on this policy 13
Appendix 1: Equality impact assessment 14
Aims, objectives and purpose of the policy 14
Differential impacts 14
Human rights values 16

Public Sector Value Act 2012 16
Equality impact assessment action plan 18

1. Introduction

It is NHS policy and a legal requirement that when patient data is used for purposes other than involving direct care, the patient should not be identified unless there is a legal basis to do so, for example explicit patient consent.

The NHS confidentiality code of practice states the need to effectively anonymise patient data prior to the non-direct care usage being made of the data.

Data itself cannot be labelled as primary or secondary use data; it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users can have identifiable data disclosed to them.

2. Purpose

This policy provides the framework for how the organisation will use patient identifiable data for purposes other than the direct care of the patient.

All Cornwall and Isles of Scilly Integrated Care board (ICB) staff must:

- Ensure appropriate changes are made to processes, systems and security mechanisms to facilitate the use of de-identified data in place of patient identifiable data
- Use the latest data security and protection toolkit (DSPT) to assist in the implementation and assessment of compliance with policy, procedural and legal requirements
- Ensure that relevant staff are aware of the requirements and are trained to use anonymised or pseudonymised data unless otherwise required by the demands of their role as specified in this policy

3. Definitions

Pseudonymisation and/or pseudonymised data

Also known as de-identification, is the process involved to enable NHS organisations to undertake secondary usage of patient data in a legal, safe and secure manner.

Pseudonymisation involves the removing of identifiers from patient data so that a patient/service user may not be identified.

However, where multiple sets of data are used, links should be enabled so that it is possible to analyse data sets and trends over time. Individual service user activity should be able to be identified but not the service user themselves.

Anonymised Data

This is information which does not identify an individual directly and which cannot reasonable be used to determine identity.

Anonymisation does not allow information about the same individual to be linked in the same way that pseudonymisation does and is more likely to be used for “one-off queries” of data.

Primary use

Primary use of patient data covers two types; those that directly contribute to the diagnosis, care and treatment of an individual and those used in the audit/assurance of the quality of healthcare provider.

Secondary use purposes

Where patient identifiable data (PID) is used for work not directly related to the care of the patient/service user.

Examples of secondary uses are commissioning, payment by results (PbR), performance management, capacity planning, service redesign and benchmarking.

Personal confidential data (PCD)

PCD essentially refers to any data or combination of data that can be used to identify an individual.

These include but are not limited to the following:

- Name – including last name and any forename or aliases
- Address – including any current or past address of residence
- Date of Birth
- Postcode – including any current or past postcode of residence
- NHS number
- Ethnic category
- Local patient identifier
- Patient pathway identifier
- SUS spell ID
- Unique booking reference number
- Social service client number
- Date of death

Confidential patient identifiable data

One or more of the data items specified in the list above that can be viewed unmodified allowing:

- Patients to be identified and differentiated within any subset of data
- Patient records to be linked across systems

Non-confidential patient data – Pseudonymised

One or more of the data items specified in the list above that can be viewed unmodified allowing:

- Patients to be identified only via secure, caldicott approved and managed access to related confidential patient identifiable data
- Patients to be differentiated within any subset of data
- Patients to be linked across systems

Non-confidential patient data - Part-anonymised

One or more of the data items specified in definition of “PCD” above that can be viewed/modified:

- Allowing patients to be differentiated within any subset of data but not identified via other data sources and not allowing
- Patients to be linked across systems or subsets of data

Non-confidential patient data - Fully anonymised

None of the data items specified in the definition of “PCD” can be viewed allowing:

- Differentiation by activity codes only – no patient differentiation or identification or linkage across systems or subsets of data.

4. Responsibilities

Chief executive

The chief executive has overall responsibility for the Data Protection Act (DPA) 2018. The development, implementation of and compliance with this policy is delegated to the director of transformation and partnerships who is also the SIRO.

Senior information risk owner (SIRO)

The SIRO is responsible for the management of information risk, with a particular focus on information asset management. The SIRO is the executive lead for pseudonymisation.

Caldicott guardian

The caldicott guardian will oversee all disclosures or change processes that involve the collection of individual personal information. The caldicott guardian must review and authorise staff access to PCD for secondary use purposes.

Head of information governance

The head of information governance is the named Data Protection Officer for the ICB in accordance with the Data Protection Act 2018 and chairs the information governance sub-committee.
The role of head of information governance includes:

- overseeing the policies and procedures required to ensure compliance with the Data Protection Act 2018 and subsequent regulations
- overseeing the ICB data security and protection toolkit (DPST) submission and ensuring all mandatory requirements are achieved.

Managers

Managers must:

- identify staff that have a justified purpose to access PCD for secondary use purposes
- ensure staff undertake annual mandatory online information governance/data security and awareness training
- regularly review the appropriateness of staff access to PCD
- organise the removal of staff access rights to PCD, where there is no longer a need for staff to access PCD for secondary use purposes
- inform the head of information governance of new staff that require access to PCD for secondary use purposes

Staff

Staff with access to PCD for secondary uses purposes must:

- keep PCD confidential
- only use/transfer PCD when authorised to do so
- transfer PCD in a secure manner as per the safe haven guidelines
- when transferring PCD via email to another NHS organisation, NHS mail should be used by both sender and recipients
- when transferring PCD via email it should not be included in the main body of the email but attached as a secure document and marked as confidential
- all other transfers of PCD should be via approved secure methods and/or secure networks
- anonymise PCD where possible and, in all cases, use the minimum amount of PCD necessary used (see caldicott principles for further details)

5. General principles

PCD should generally only be used where:

- there is a direct care-related need to use such data. Patient level data should not contain identifiers when they are used for purposes other than the direct care of patients.
- patient consent has been received (or there is another lawful basis for doing so under the Data Protection Act 2018)

When using PCD for secondary use purposes, data must be anonymised or de-identified as much as practically possible.

Data itself cannot be labelled as primary or secondary use data; it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users can have identifiable data disclosed to them.

Safe haven procedures must be always used when handling and sharing PCD, regardless of whether the data is being used for healthcare purposes or secondary uses purposes.

Staff who have access to PCD for secondary purposes should be identified. Access to PCD for secondary purposes should be appropriately authorised by the head of information governance/data protection officer or the caldicott guardian.

A register of staff with access to PCD for secondary uses purposes should be created and maintained.

Even when it is legally permissible to use person identifiable information, its use should be minimised, for example by only sending a relevant subset of the information or using one or more of the techniques described in the guidance. This is in line with the caldicott principles.

Pseudonymisation

Pseudonymisation is the process of distinguishing identities. The aim of such a process (vs anonymisation) is to be able to collect additional data relating to the same individual without having to know the identity.

Pseudonymisation can be likened to anonymised information in that in the possession of the holder it cannot reasonably be used by the holder to identify an individual. However, it differs in that the original provider of the information may retain a mean of identifying individuals.

This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index. Pseudonymisation allows information about the same individual to be linked in a way that true anonymisation does not.

Key-coded data is an example of pseudonymisation. This applies to all electronic patient identifiable data, from large databases with thousands of records down to documents or files holding a single item of data, except those used for direct care and those information flows covered by section 251 regulations for public health.

To effectively pseudonymise data the following actions must be taken:

- an algorithm must be applied to the agreed data field within the patient record, for example the NHS number to generate a pseudonymised identification number to be used on reports from secondary uses purposes
- each field of PCD must have a unique pseudonym
- 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 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 character, for example, “5L7 TWX 619Z” which incorporates letters within the pseudonym for an NHS number to avoid confusion with original numbers.

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.

The secondary use output must only display the pseudonymised data items that are required.

6. Pseudonymisation controls

Current pseudonymisation controls on data flowing to the ICB are NHS Digital approved tools and are applied at source by the data services for commissioners regional office (DSCRO) – see section 7 below.

7. DSCRO

The DSCRO is a service which processes data to support local commissioning whilst protecting patient confidentiality in line with the Health and Social Care Act.

The DSCRO follows strict processes to protect the confidentiality of data. Controls are in place regarding the release of data from this service. In particular, personal confidential data (PCD) will only be passed on to other health organisations if there is a lawful basis for that to happen.

Data flows out of the DSCRO will be one of the following:

- aggregate data
- pseudonymised data, supported by an appropriate data sharing and/or processing agreement
- data for direct patient care
- identifiable data supported by a relevant s251 agreement
- where patient consent has been obtained

8. Section 251 approval

The section 251 application process is very rigorous and is managed by the confidentiality advisory group (CAG). Applicants must demonstrate that the aim of processing is in the public interest, that anonymised information could not be used to achieve the required results and that it would be impractical – both in terms of feasibility and appropriateness – to seek specific consent from each individual affected. For research the approval of a research ethic committee is also needed. The test is one of necessity, not convenience.

The powers under the section 251 regulations only provide relief from the Common Law Duty of Confidentiality. Any activity taking place with the support section 251 must still comply in full with the Data Protection Act.

9. Safe havens

Safe haven procedures should be in place in any location where large amounts of personal information is being received held or communicated especially where the information is of a sensitive nature. There should be at least one area designated at Safe haven at each ICB.

10. Accredited safe havens

Accredited safe havens (ASHs) are commissioning bodies, or a designated part of an organisation which is contractually and legally bound to process data in ways that prevent the identity of individuals to whom the data relates from being identified. To maintain ASH status each ASH must provide evidence of the successful completion of the mandatory requirements within the new DSPT.

An ASH may process data that is only weakly pseudonymised. This means the data has the potential to identify an individual if handled outside the controls of the ASH environment (e.g. NHS number).

Weakly pseudonymised data may contain the NHS number or the postcode, which on its own will not directly identify the individual, but outside of the controls of the ASH would make the data identifiable.

11. Controlled environment for finance

A CEfF is either part of a commissioning support unit (CSU) or part of an ICB. It is a nominated secure environment that can receive the minimum necessary PCD to validate invoices.

Staff within the CEfF can access and view PCD to determine the relevant commissioner as part of invoice validation. They can also provide de-identified data sets for further analysis. CEfF are an innovation to assist in the resolution of invoice validation issues and are expected to be a short term solution.

12. Training requirements

All staff are required to undertake mandatory online information governance or data security and awareness training via electronic staff record on-line provision. More specialist training and support is also available with advice from the HOIG.

13. Implementation plans and monitoring effectiveness

Staff are required to report all incidents involving the loss, inappropriate destruction or unauthorised disclosure of information in line with the ICB incident reporting policies and procedures. All suspected instances generated by ICB staff will be investigated and recorded within the caldicott guardian breach log and reported to the IGSC.

The investigation of a breach may result in the commencement of formal disciplinary procedures. It should also be noted that unlawful disclosure of personal data can lead to civil proceedings against both the ICB and the individual concerned.

14. Update and review

Review of this policy will be carried out by the HOIG.

15. References, policies and legal framework

Legislation referring to issues of security and or confidentiality of person identifiable data:
Data Protection Act 2018
UK General Data Protection Regulations (GDPR)
Freedom of Information Act 2000
Computer Misuse Act 1990
Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
Crime & Disorder Act 1998
The Directive on Privacy and Electronic Communications (2002/58/EC)
Electronic Communications Act 2000
Regulation of Investigatory Powers Act 2000
Lawful Business Practice Regulations 2000
Criminal Justice & Court Services Act 2000 (where Multi Agency Public Protection Panels & Information exchange is set out)

Legislation to restrict disclosure of personal identifiable information:

Human Fertilisation and Embryology (Disclosure of Information) Act 1992
Venereal Diseases Act 1917 and Venereal Diseases Regulations of 1974 and 1992
Abortion Act 1967
The Adoption Act 1976

Legislation requiring disclosure of personal identifiable information:

Public Health (Control of Diseases) Act 1984 & Public Health (Infectious Diseases) Regulations 1985
Education Act 1944 (for immunisations and vaccinations to NHS Trusts from schools)
Births and Deaths Act 1984
Police and Criminal Evidence Act 1984
Health and Social Care (Safety and Quality) Act 2015

Additionally, the NHS has mandated a number of relevant regulations including:

DSPT
Caldicott report 1998 and subsequent reviews and reports
International standards organisation standard for information security management,
Data quality assurance to include NHS data dictionary, hospital episode statistics (HES) and mental health minimum data set (MHMDS)
Confidentiality: NHS code of practice
NHSX records management code of practice
Information security management: NHS code of practice
BS10012:2009 Data Protection: specification for a personal information management system
The NHS constitution

16. Consultation on this policy

Consultation on this policy took place originally with the business intelligence team, corporate governance team and the IGSC. The policy was circulated in the staff bulletin and made available to staff in the document library. The policy was ratified at senior management team in February 2019 and reviewed in January 2023.

Appendix 1: Equality impact assessment

Name of policy or service to be assessed: Pseudonymisation policy
Department or section: Information governance
Date of assessment: January 2023
Person(s) responsible for the assessment: Head of information governance
Is this a new or existing policy? Existing

Aims, objectives and purpose of the policy

Describe the aims, objectives, and purpose of the policy.
This policy provides a framework by which the ICB will ensure the provision of robust information governance management arrangements to meet its legal and regulatory responsibilities. The policy details the ICB commitment to meet its obligations in the protection of person identifiable data and sensitive business data whilst also recognising the need to share information by secured methods

Who is intended to benefit from this policy, and in what way?
ICB staff from the implementation of robust information security controls to protect them and the information they process as part of the services provided. Patients will benefit ultimately from the provision and availability of high quality information and data which meets the NHSX records management code of practice.

What outcomes are wanted from this policy?
That the information processed by the ICB, in all formats, is protected to the highest possible standards and available quickly, processed in line with legislation and all confidentiality requirements, government standards and health and social care information centre requirements

What factors or forces could contribute or detract from the outcomes?
Lack of staff awareness of the policy. Lack of availability of robust technical or procedural controls to protect information. Lack of resources to implement all the actions identified.

Who are the main stakeholders in relation to the policy?
The ICB board in meeting its responsibilities. Staff processing information in all types of formats. All contractors processing information on behalf of the ICB.

Who implements the policy, and who is responsible for the policy?
The IGSC and HOIG.

Differential impacts

Does this have a positive or negative impact on people from an ethnic minority background? How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of ethnicity. There are no negative impacts.

Does this have a positive or negative impact on people who identify as male, female or intersex? How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of whether individuals identify as male, female or intersex. There are no negative impacts.

What is the positive or negative differential impact on people from the perspective of disability? How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of whether individuals are disabled. There are no negative impacts.

Does this have a positive or negative impact on people who identify as heterosexual, lesbian, gay, bisexual, pansexual or asexual? How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of whether individuals identify as heterosexual, lesbian, gay, bisexual, pansexual or asexual. There are no negative impacts.

What is the positive or negative differential impact on people from the perspective of age? How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of age. There are no negative impacts.

What is the positive or negative differential impact on people from the perspective of religion or belief? How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of religion or belief. There are no negative impacts.

What is the positive or negative differential impact on people from the perspective of marriage and civil partnership? This is particularly relevant for employment policies. How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of marital status. There are no negative impacts.

Does this have a positive or negative impact on people who identify as trans or transgender, non-binary, or gender fluid? How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of gender. There are no negative impacts.

Does this have a positive or negative impact on people who are pregnant, breast feeding mothers, or those on maternity leave? How will any negative impact be mitigated?

The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals, irrespective of whether they are pregnant, breast feeding mothers, or on maternity leave. There are no negative impacts.

Are they any other identified groups? How will any negative impact be mitigated?
The policy reflects the current national guidance and best practice and is designed to protect the rights of all living individuals. There are no negative impacts.

Human rights values

How have the core human rights values of fairness, respect, equality, dignity, and autonomy been considered in the formulation of this policy, service, or strategy?
The Act has been referenced within the information governance policies and procedures produced and any monitoring of compliance will include the awareness of patients and staff having a right to privacy, dignity, respect and choice. Training in Human Rights Act is also made available to staff.

Which of the human rights articles does this document impact?

☐ To life
☐ Not to be tortured or treated in an inhuman or degrading way
☐ To liberty and security
☐ To a fair trial
☒ To respect for home and family life, and correspondence
☐ To freedom of thought, conscience, and religion
☐ To freedom of expression
☐ To freedom of assembly and association
☐ To marry and found a family
☐ Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention
☐ To peaceful enjoyment of possessions

What existing evidence (either presumed or otherwise) do you have for this?
All information governance policies are linked to the Human Rights Act with regard to privacy and dignity.

How will you ensure that those responsible for implementing the policy are aware of the human rights implications and equipped to deal with them?
All information governance policies are linked to the Human Rights Act with regard to privacy and dignity. Staff are expected to complete annual mandatory data security and protection training which incorporates individual information rights.

Public Sector Value Act 2012

NHS Cornwall and Isles of Scilly is committed and obliged to fulfil the requirements of the Public Sector Social Value Act 2012. This Act requires the organisations to

consider how services commissioned or procured might improve the economic, social, and environmental wellbeing of an area.

Please describe how this will support and contribute to the local system, wider system, and community.
This policy describes the services provided to the ICB by DSCRO who pseudonymise data on behalf of many NHS organisations to comply with data protection, UK GDPR and confidentiality legislation. This data allows the ICB to monitor and plan provider service to make best use of resources in Cornwall and Isles of Scilly.

Describe how the policy contributes towards eliminating discrimination, harassment, and victimisation.
All personal identifiers are removed from the data processed by the ICB and therefore no discrimination would be possible as only statistical data remains.

Describe how the policy contributes towards advancing equality of opportunity.
All personal identifiers are removed from the data processed by the ICB but in some instances it may be possible to identify and report on groups of individuals who may not take up services in line with others. As the data is statistical there is potential to recognise any gap and work towards improving those services.

Describe how the policy contributes towards promoting good relations between people with protected characteristics.
All personal identifiers are removed from the data processed by the ICB but in some instances it may be possible to identify and report on groups of individuals who may not take up services in line with others. As the data is statistical there is potential to recognise any gap and work towards improving those services.

If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services and or the working environment for that group of people.
All personal identifiers are removed from the data processed by the ICB but in some instances it may be possible to identify and report on groups of individuals who may not take up services in line with others. As the data is statistical there is potential to recognise any gap and work towards improving those services.

Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.
No amendments have been made to the policy as no negative or differential impacts are recognised within.

If the negative impacts identified have been unable to be mitigated through amendment to the policy or other mitigating actions, explain what your next steps are using the following equality impact assessment action plan.
No negative or differential impacts are recognised in the policy and therefore no action plan is necessary.

Equality impact assessment action plan

Issue to be addressed	Action required	Responsible person	Timescale for completion	Action taken
N/A	N/A	N/A	N/A	N/A

Comments on action plan:
N/A

Signed (completing officer): Head of information governance

Date: January 2023

Signed (head of department or section): Head of information governance

Date: January 2023

Please ensure that a signed copy of this form with the policy is sent to both the corporate governance team and equality and diversity lead.