BrisDoc Patient care by people who care

NHS

Data Sharing with 3rd Parties Pseudonymisation and Anonymisation Policy

Version:	Owner:	Created:
1.51	Debs Lowndes (Head of Business Information and Systems.)	1st March 2014
Published:	**Approving Director:**	**Next Review**
17/04/2025	Rhys Hancock (Director of Nursing, AHPs and Governance)	17/04/2027

Contents

1. Introduction 3
2. Legal Requirements 3
3. Accountability and Staff Responsibilities 3
4. De identification aims 4
5. Personal Identifiers 4
6. Guidance of De-identification 5
7. Cybersecurity and Data Protection Considerations 5
8. Unsure what to Do 6
Appendix A Information Sharing Agreement Template 7
9. Tables 7

Data Sharing with 3rd Parties Pseudonymisation and Anonymisation Policy V1.51

1. Introduction

The purpose of this policy is to provide guidance when preparing data extracts to share with third parties, to ensure that the secondary use of patient data is done so in a legal, safe and secure manner e.g. ICB, partners and universities/health bodies for research purposes.

All such requests should be documented as an **Information Request** and be reviewed and signed-off by the CG, SIRO or ISM before being sent. The output of the review i.e. what dataset is agreed should be sent and any restrictions to be applied should be recorded as part of the request in the Information Request register.

An information sharing agreement might be applied where there is regular sharing of data, see template in appendix A. This form should be completed and required and signed off by the SIRO and/or CG SIRO as appropriate.

2. Legal Requirements

It is a legal requirement that when patient data is used for purposes not involving the direct care of the patient, i.e. Secondary Uses, the patient should not be identified unless other legal means hold, such as the patient's consent or Section 251 approval. is only required when processing identifiable patient data without explicit consent.

Where there is a doubt or processing high-risk data-sharing activities a Data Protection Impact Assessment (DPIA) should be completed refer to the Data Protection by Design Policy for further guidenance.

This is set out clearly in the NHS policy and good practice guidance 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.

Data 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 even where it is justifiable to hold data in identifiable form, it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them.

3. Accountability and Staff Responsibilities

- The following roles are accountable for overseeing and enforcing compliance of this policy;
- Senior Information Risk Owner (SIRO) – Responsible for managing information risks associated with data sharing, ensuring that risks are identified, assessed, and mitigated. The SIRO must approve all high-risk data-sharing activities.
- Caldicott Guardian (CG) – Ensures that any sharing of patient-identifiable information is justified, follows the Caldicott Principles, and upholds patient confidentiality.
- Data Protection Officer (DPO) – Provides advice on UK GDPR compliance, assesses Data Protection Impact Assessments (DPIAs) for high-risk data-sharing projects, and acts as the main point of contact for regulatory authorities (e.g., ICO).
- Service/Function Information Governance Lead(s) – responsible for the recording of all data sharing agreements and following the appropriate IG policies to ensure safe sharing is achieved.

- Digital Team – Ensures technical security controls, such as encryption, access management, and cybersecurity monitoring, are in place for data sharing as required.
- All Staff Handling Shared Data – Must follow the Data Sharing Policy, complete mandatory information governance training, and report any potential data breaches or security concerns to the IG Lead or SIRO.
- All data-sharing activities must be authorised, documented, and regularly reviewed to ensure compliance. Any failure to follow these responsibilities may result in disciplinary action or a review of access privileges.

4. De identification aims

There is an overarching Information Governance principle that users 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 1, 2 and 3.

This principle applies to the use of patient level data for secondary or non-direct care purposes. The utilisation of de-identification tools enables users to make use of patient level data for a range of secondary purposes without having to access those data items, which may reveal the identity of the patient.

The aim of de-identification is to obscure person/patient identifier data items and combinations of them within patient records sufficiently that the risk of potential identification of the subject of a patient record is minimised to acceptable levels to be regarded as 'effective anonymisation'.

It should be noted that the risk of identification can never be totally eliminated. This is because a particular user of data may be familiar with individuals with specific or unique characteristics and therefore be able to identify them, or selecting such individuals combined with additional research could achieve identification through use of inference techniques. The use of de-identification tools does not replace the general requirement to restrict access to data to that needed for a particular purpose. It should be complimentary. For example, if a report or piece of business analysis is undertaken as a monthly time series, there may be no need for users to access the full date of admission or discharge of a patient.

All organisations and individuals should be aware of their responsibilities to respect patient confidentiality and comply with the law, as embodied in Caldicott Principles 5 and 6 and the NHS Code of Practice on Confidentiality.

5. Personal Identifiers

Those data items within patient activity data that are considered to be sensitive are based on the rules laid down for the operation of the Secondary Uses Service (SUS).

Those data items that may lead to identification of individuals can be grouped and shown (with examples but not limited to), as below:

- Strong identifiers – :
    - name
    - address
    - postcode

- Weak or indirect identifiers:

- supporting personal information – date of birth, ethnicity, sex
- operational reference numbers with meaning within the NHS - NHS Number, local patient identifier
- The fields considered as 'sensitive' in relation to identifying patients in SUS are:
    - Patient Name
    - Patient Address
    - Patient Date of Birth
    - Patient Postcode
    - Patient NHS Number
    - Patient Ethnic Category
    - Patient Local Patient Identifier
    - Patient Hospital Spell Number
    - Patient Pathway Identifier
    - Patient Unique Booking Reference Number
    - Patient Social Service Client Identifier.

In addition, if the record is for a baby or a mother, the relevant fields contained in the record for the mother or baby respectively for name, address, date of birth, postcode and NHS Number are regarded as sensitive as well. If concatenated forms of names or addresses are held in any fields, these should also be regarded as sensitive.

Additional potentially sensitive fields associated with SUS and Commissioning Data Set (CDS):

- Date of death – this is a data item not explicitly output in CDS but can potentially be derived from method and date of discharge fields for hospital patients, and is potentially held within local systems. This is also regarded by ECC as sensitive, as it may lead to ready identification of individuals. The Data Protection Act does not apply to deceased persons, but the duty of confidence continues after a patient has died.

6. Guidance of De-identification

The following table describes the actions to be taken in respect of each data item when preparing data extracts for 3rd Party sharing.

Data Item	Action to be Taken
Name	Do not display
Address	Do not display
Postcode	Display the First 3 or 4 Chars
Contact Numbers	Do not display
Date of birth	Replace by age in years
NHS Number	Pseudonymised or do not display
Ethnic category	Identifiable if relevant to report, otherwise do not display
Local patient	Pseudonymised or do not display Identifiable

7. Cybersecurity and Data Protection Considerations

BrisDoc recognises the critical importance of cybersecurity in safeguarding patient data when sharing information with third parties. All data transfers must adhere to this policy, the NHS Data Security and Protection Toolkit, and relevant UK GDPR requirements. To ensure data security:

- Encryption: All patient data shared electronically must be encrypted using NHS-approved encryption standards (e.g., AES-256).
- Secure Transfer: Data must only be transferred via approved, secure methods, such as NHSmail, secure file transfer protocols (SFTP), or an encrypted cloud service compliant with ISO 27001.
- Access Controls: Only authorised personnel with a legitimate need-to-know basis should have access to shared data. Multi-factor authentication (MFA) and role-based access controls (RBAC) should be implemented.
- Audit and Monitoring: All data access and transfers must be logged and monitored to detect unauthorised access or suspicious activity.
- Incident Response: Any suspected data breach or cybersecurity incident must be reported immediately to the Information Governance Lead, SIRO, and IT Security Team, following BrisDoc's Incident Response Plan. If required, incidents will be reported to the ICO within 72 hours.

Failure to adhere to these security measures may result in disciplinary action and a review of data-sharing agreements.

8. Unsure what to Do

Please seek advice from Senior Information Risk Officer (SIRO) if you are unsure before you release any information.

Appendix A Information Sharing Agreement Template

The link to the NHS template DSA is here:

https://transform.england.nhs.uk/information-governance/guidance/universal-ig-templates-faqs/

9. Tables

Date	Reviewed and amended by	Revision details	Issue number
March 2014	DL		DRAFT
February 2015	DL	First full version for review	1.0
February 2017	DL	Annual review, additional appendix A for completeness	1.1
February 2019	DL	Annual review no changes	1.2
February 2021	DL	Annual review no changes	1.3
February 2023	DL	Annual review no changes	1.4
March-2025	DI	Annual review and change of SIRO	1.51