BrisDoc Patient care by people who care

NHS

Data Sharing with 3rd Parties Pseudonymisation and Anonymisation Policy

Version:	Owner:	Created:
1.4	Debs Lowndes (Head of Business Information and Systems.)	1st March 2014
Published:	**Approving Director:**	**Next Review**
15th November 2023	Nigel Gazzard (Managing Director.)	1st February 2025

Contents

Policy

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 DAC

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 ISM, CG and 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.

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. 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 so as 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.

4. 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 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.

5. 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

6. Unsure what to Do

Please seek advice form the IG Lead Debs Lowndes or Senior Information Risk Officer (SIRO) Nigel Gazzard if you are unsure before you release any information.

Appendix A Information Sharing Agreement Template

Information Sharing Agreement (ISA)

This Information Sharing Agreement (ISA) defines the arrangements for processing data between Brisdoc Healthcare Services and <XYZ>.

1. Parties to the agreement: Full name and address of the organisations or businesses

BrisDoc Healthcare Services Unit 21 Osprey Court Whitchurch Lane Bristol BS14 0BB And

2. Why is the information being shared?

3. What information being shared?

4. What is your legal justification for sharing? Has consent been gained if required?

5. How will the information be shared? (e.g. data transfer - include any security measures)

6. How will the information be stored? (e.g. secure server - include any security measures)

7. Who will handle the information – name and job title?

8. How long will the information be kept?

9. How will the information be destroyed?

10. What date will the information be shared? Initial date must be later that the date of the signatures below and should give an indication of subsequent dates for regular sharing.

11. What are the names, roles and contact details of any members of staff who will make sure that the required information is shared at the appropriate time?

12. When will this agreement be reviewed and by whom?

This agreement must be formally approved and signed by both parties before any information sharing takes place. Both parties will ensure that the ISA and any associated documents are known and understood by all staff involved in the process.

Should an incident arise executing this process as a result of this process, each organisation will use their standard incident reporting process and make the other organisation aware of the incident.

Originating Organisation
Name of organisation: BrisDoc Healthcare Services
Name: Deb Lowndes
Position: Head Of Business Information and Projects

Signature	Date:

Partner Organisation
Name of organisation: <XYZ>
Name:
Position:

Signature	Date:

7. 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