NHS
Business Services Authority

Pseudonymisation and anonymisation of data policy

Issue sheet

Document reference	NHSBSAPA001
Document location	
Title	NHS Business Services – Pseudonymisation and anonymisation of data policy
Author	Chris Chester
Issued to	All NHSBSA staff
Reason issued	For information / action
Last reviewed	27 April 2015

Revision details

Version	Date	Amended by	Approved by	Details of amendments
Version 2	18.02.2015	C Gooday	ISF	Caldicott 2 report and clarity on use of identifiers

Contents

1. Introduction

A fundamental principle of the Data Protection Act 1998 is to use the minimum personal data to satisfy a purpose and to strip out information relating to a data subject that is not necessary for the particular processing being undertaken. This principle is aligned with the Caldicott Principles familiar to NHS and Social Care organisations and is supported by both common law confidentiality obligations and the Human Rights Act 1998 which provides a privacy right for individuals.

There is also a requirement that organisations respect people's private lives unless there is a lawful exemption to the Human Rights requirements and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned.

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 a part of the organisation designated as a 'safe haven' where it can be processed securely and only used in an identifiable form for specific authorised procedures within the safe haven boundary. Onward disclosure should be limited to pseudonymised or anonymised data.

Effective pseudonymisation and/or anonymisation processes depend upon robust information governance and effectively trained staff who understand the importance of data protection and confidentiality.

2. Scope

This policy is specifically concerned with the security of patient level clinical data when used for purposes other than direct patient care including, but not limited to:

- Pensions Injury Benefit;

- HR Occupational Health Records;
- Etc.

This policy is in line with the NHS Operating Framework 2011/12.

3. Purpose

This document seeks to provide all NHSBSA personnel who use patient level clinical data with guidance to safeguard the confidentiality when the data is used for purposes other than direct patient healthcare.

4. Definitions

- Personal Identifiable Data (PID) – is any information that can identify one person. This could be one piece of data for example a person's name or a collection of information for example name, address and date of birth.
- Primary Uses – is when information is used for healthcare and medical purposes. This would directly contribute to the treatment, diagnosis or the care of the individual. This also includes relevant supporting administrative processes and audit/assurance of the quality of healthcare service provided.
- Secondary Uses – is for non-healthcare and medical purposes. Generally this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When PID is used for secondary use this should, where appropriate, be limited and de-identified so that the secondary uses process is confidential.

5. Responsibilities

Ultimately responsibility for this Policy rests with the NHSBSA Leadership Team, but on a day-to-day basis the Information Governance and Security Group (IGSG) and the NHSBSA Head of Internal Governance (HoIG) role within the NHSBSA will be responsible for managing and implementing the Policy.

The HoIG is responsible for ensuring that the designated training in areas of Data Protection and Information Security cover Anonymisation and Pseudonymisation.

All staff are responsible for compliance with the policies and procedures as well as identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising the IGSG accordingly.

6. Business processes

All business processes, using patient level clinical data, within the NHSBSA must be documented. Business processes can include, but are not limited to:

- the process for using patient data for secondary uses;
- the use of PID for a combination of primary and secondary.

Primary use includes, but is not restricted to the patient treatment details or inputting test results. All information recorded about a person should be recorded in line with the NHSBSA's Records Management Policy and the Data Protection Act 1998.

Secondary use business processes should be initially documented and then reviewed regularly to assess any requirement to use de-identified data. Following assessment any processes that require de-identified data must be modified in line with this policy.

All onward disclosure should be limited to pseudonymised or anonymised/de-identified data.

7. Anonymisation / de-identification

Staff only have access to the data that is 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 patient level clinical data for a range of secondary purposes without having to access the identifiable data items.

The aim of de-identification is to obscure the identifiable data items within the persons records sufficiently that the risk of potential identification of the subject or a persons record is minimised to acceptable levels, this will provide effective anonymisation. Although the risk of identification can not be fully removed this can be minimised with the use of multiple pseudonyms.

De-identified data should still be used within a secure environment with staff access on a need to know basis.

De-identification can be achieved by:

- Removing direct patient identifiers;
- The use of identifier ranges, for example; value ranges instead of age;
- By using a pseudonym.

If patient data is required the NHS Number is the most secure form of identifiable data. 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

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

To effectively pseudonymise data the following actions must be taken:

- Each identifying field of PID must have a unique pseudonym;
- Pseudonyms to be used in place of NHS Numbers and other fields 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;
- 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;
- Where used pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised;
- The secondary use output must, where pseudonyms used, only display the pseudonymised data items that are required. This is in accordance with the Caldicott Guidelines;
- Pseudonymised data should have the same security as PID.

9. Use of identifiable data

If patient records are viewed in an identifiable form then the reasons and usage of the data should be fully documented and approval is required by the appropriate data owner. This auditable trail of access to patient's records supports the Care Record Guarantee where patients are to be informed as to who has accessed/seen their data and the audit will provide accurate data in the event of untoward incidents.

The key items to be documented are:

- Who has accessed each data base containing identifiable data;
- Date and time of access;
- The reason for the access;
- The output from the access.

This audit should be kept within a separate structured database to enable queries and audit.

The log of accesses must be regularly audited via sampling of users or subject matter to check for unusual patterns of access. If any unusual patterns of access are noted this should be reported via the IGSG.

10. Transferring information

Appropriate data sharing agreements should be in place when information is to be transferred to another organisation.

If the transfer of information is required for secondary use then a form of anonymised or pseudonymised data should be sent.

11. Legal and professional obligations

All NHS records are Public Records under the Public Records Act. The NHSBSA will take actions to comply with the relevant legal and professional obligations, in particular:

- The Caldicott Principles;
- Data Protection Act 1998;
- Human Rights Act 1998;
- Common Law duty of Confidentiality;
- NHS Operating Framework 2011/12; and
- The NHS Confidentiality Code of Practice.

12. Training

All NHSBSA staff will be made aware of their responsibilities relating to this policy through generic and specific training programmes and guidance.

13. Validity of this policy

This Policy is designed to avoid discrimination and be in accordance with the Human Rights Act 1998 and its underlying principles.

This Policy should be reviewed annually under the authority of the NHSBSA Executive Board members. Anonymisation and pseudonymisation standards should be subject to an ongoing development and review programme.

14. References

- NHS Connecting for Health IG Toolkit
- NHS Operating Framework 2011/12
- Caldicott Committee Report 2012