The Tavistock and Portman
NHS Foundation Trust

Pseudonymisation and Anonymisation of Data - Procedure

Version:	V1.0
Bodies consulted:	IG Workstream
Approved by:	Executive Management Team
Date Approved:	8 January 2019
Lead Manager	Data Security and Protection Manager and DPO
Responsible Director:	Senior Information Risk Owner (Deputy CEO and Director of Finance)
Date issued:	11 January 2019
Review date:	December 2023
Intranet	Yes
Extranet	Yes

Contents

1 Introduction 4
2 Definitions 4
3 Purpose 5
4 Scope 5
5 Governance, roles and responsibilities 5
6 Pseudonymisation and Anonymisation Guidance 6
6.1 Processing data 6
6.2 Pseudonymised data 6
6.2.1 Security 7
6.2.2 Data Sharing Agreement 7
6.3 Anonymised data 7
6.4 Approved research projects 7
6.5 Further guidance 8
7 Risk Assessment 8
8 Pseudonymisation and Anonymisation Controls 8
8.1 Data Flow Mapping 8
8.2 Access to Person Identifiable Data 9
9 Distribution and implementation 9
10 References and resources 9
Appendix 1 11

1 Introduction

This Procedure provides the framework for how Tavistock and Portman NHS Foundation Trust ("Trust") will manage the use of patient identifiable data for purposes other than the direct care of patients.

Its implementation and adherence will support compliance with legislation and best practice; a number of Data Security and Protection Toolkit ("DSPT") assertions; and the Trust Pseudonymisation Implementation Project Plan.

2 Definitions

Personal Identifiable Data (PID)
Any information that can identify an individual. 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
When information is processed 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
When information is processed for non-healthcare and medical purposes. Generally, this could be for research purposes, audits, service management, commissioning, contract monitoring and reporting facilities.
Processing data
Processing can mean gathering, using, holding, storing, disclosing, transferring, destroying – anything to do with data.
Anonymised
Anonymisation is the process of turning data into a form which does not identify individuals and where identification is not likely to take place. It is important to ensure that anonymisation is conducted effectively and that the data cannot be matched with other data and allow re-identification.
Aggregate data
Data derived from records about more than one person and expressed in summary form, such as statistical tables.
Pseudonymised data
Pseudonymised (or key-coded) data is where a unique identifier is used to disguise the personal identity but which can be tracked back by the person who has the 'key'
Section 251
Section 251 (of the National Health Service Act 2006 and its current Regulations – the Health Service (control of Patient Information) Regulations 2002 - may be used by organisations that have obtained approval from the Secretary of State to use specific confidential information for non- direct-care purposes. The Regulations allow the common law duty of confidentiality to be set aside for medical purposes where anonymised data cannot be used and where obtaining the consent of the individuals concerned is impractical.

3 Purpose

A fundamental principle of the Data Protection Legislation - General Data Protection Regulation ("GDPR") and Data Protection Act 2018 ("DPA") - is to use the minimum personal data required for the task in hand. This principle is aligned with the Caldicott Principles and is supported by the common law confidentiality obligations, the Human Rights Act 1998 and 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 use for non-healthcare medical purposes.

The purpose of this document is to provide guidance to staff so that:

- Personal Identifiable Data ("PID") is processed legally and securely
- It is clear when data should be pseudonymised or anonymised
- Staff know how to pseudonymise or anonymise data
- Business processes continue to be effective in supporting the day to day operation of the Trust's business
- Staff know where to seek advice.

4 Scope

All Trust staff must follow this guidance.

5 Governance, roles and responsibilities

The Chief Executive is accountable for information and delegates responsibility for the management of information risk to the Senior Information Risk Owner ("SIRO") and Information Asset Owners ("IAOs") who have specific responsibilities. The Data Security and Protection Manager and DPO is responsible for ensuring that a framework for proper governance and assurance is in place.

All staff are responsible for abiding by this guidance and, in discharging their duties in accordance with the law, ensuring that the confidentiality and security of information in all formats is maintained and that any disclosure is appropriate and provided to the correct contact point. In this, they are supported by the procedures, best practice guidance and the Trust Information Governance, Data Security and Protection policies and procedures.

Failure to comply with the standards and appropriate governance of information, as detailed in this Procedure, could result in disciplinary action. Staff are also reminded that this Procedure covers several aspects of legal compliance and failure to maintain these standards could result in criminal proceedings against the individual. These include but are not limited to:

- General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990

6 Pseudonymisation and Anonymisation Guidance

6.1 Processing data

Person Identifiable Data ("PID") may only be processed:

- For Primary Uses (i.e. direct healthcare purposes)
- Where the patient's explicit consent to process PID has been gained
- Where the processing of PID is covered by legislation
- In exceptional circumstances, where processing is justified in the public interest
- Where a Section 251 approval has been gained for the processing of PID.

Where data is to be used for Secondary Uses (i.e. non-healthcare medical purposes), and there is no legal basis to disclose PID, data must be pseudonymised or anonymised.

See Appendix 1 for guidance diagram.

6.2 Pseudonymised data

Pseudonymised (or key-coded) data is used to mask the identity of patient data when it is shared with persons for secondary uses. A unique identifier is used and only those with the 'key' can track back to the patient's details.

A typical pseudonymisation will replace the NHS number with an alternative unique number.

Pseudonymisation Notes:

The use of NHS Numbers as the unique identifier is not generally acceptable as this is considered 'weak' pseudonymisation in that there is the potential to easily re-identify an individual. Staff should seek advice from the Data Security and Protection Manager & DPO before pseudonymising data by means of the NHS number.

- It should be borne in mind that it may be possible to re-identify patients by a rare disease or particular set of circumstances.

Data which includes the date of birth and the postcode is not acceptable pseudonymisation.

- Dates of birth are difficult to pseudonymise because of the very limited range - replace with age, or month and year, or use age bands.
- Postcodes can be too specific, replace with postal town, or the first part of the postcode only.

Ethnic data is classified as sensitive data and should only be displayed where it is relevant to the purpose of the data gathering.

Seek advice from the Data Security and Protection Manager regarding:

- Data relating to patients of less than 13 year of age
- Data covered by the Human Embryology Act and STD Directives, as records should be anonymised in such cases
- Using the date of death.

6.2.1 Security

Pseudonymisation is not a method of anonymisation. Pseudonymised data must be treated as PID and be secured appropriately.

6.2.2 Data Sharing Agreement

A data sharing agreement should be in place when pseudonymised information is to be transferred to a third party. The Data Processor Agreement template is available on the Trust intranet.

6.3 Anonymised data

Anonymisation is the process of turning data into a form that does not identify individuals and where identification is not likely to take place. This allows for a much wider use of the information. An example is where data has been aggregated.

Staff must follow the Anonymisation Standard for Publishing Health and Social Care Data (https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections).

This Standard is consistent with the Information Commissioner's Office Anonymisation Code (https://ico.org.uk/media/for-organisations/documents/1042731/anonymisation_code_summary.pdf)

Anonymisation Notes:

Staff must bear in mind that if a data set relates to the whole of England there will be no risk, or negligible risk, of a person's identity being revealed; however, if the data set is broken down, for example by geographical area, the risk may be such that disclosure control is required.

If there is very little or no possibility that a person could be identified from the data set, then it is not classed as personal data.

6.4 Approved research projects

Anonymised data used for ethically approved projects, where all identifying information has been removed, does not require patient consent as it cannot be linked back to an individual.

If pseudonymised data is shared with researchers, staff must ensure that there is a contractual agreement covering data flow, purposes of use, and safeguards.

6.5 Further guidance

The Data Security and Protection Manager can provide further guidance on pseudonymisation and anonymisation of data and may call upon the support of the Caldicott Guardian who takes the lead in patient confidentiality issues.

7 Risk Assessment

It is important to undertake a risk assessment when determining the data to be released prior to publishing, disclosing data to specific recipient(s), or responding to a Freedom of Information Act request.

Assessing the likelihood that personal identity could be revealed is an essential step in meeting the requirements of the law.

Risk Assessment Notes:

Staff should consider:

- The information that is already available that might be used in conjunction with the data to be released to reveal identity
- The information that may become available in future that might be used in conjunction with the data to be released to reveal identity
- The evolving use of technology which could be used to re-identify the data
- Whether there may be people who are motivated to try to discover the identity of individuals within the information to be published
- Potential value of the data to be released for those who might use it to reveal identity (if it were possible)

8 Pseudonymisation and Anonymisation Controls

8.1 Data Flow Mapping

The Trust uses data protection impact assessment (“DPIA”) and data flow mapping procedures to monitor the legal use of PID.

Where new or changed processing of PID is proposed, staff must undertake a DPIA and document the new or changed data flows.

This Pseudomymisation and Anonymisation Procedure should be read in conjunction with the DPIA to ensure the legal processing of PID.

8.2 Access to Person Identifiable Data

The Trust uses its data flow mapping process to monitor its information assets and access to person identifiable data.

Information Asset Owners must be aware of those persons who have access to their information assets, as well as the reasons for their access.

Those assets which require a Smartcard have additional security procedures including Registration Authority requirements and a regular review by Managers of the access controls granted to staff, in order to provide assurance for the legal processing of PID.

9 Distribution and implementation

These guidelines will be disseminated by the following methods:

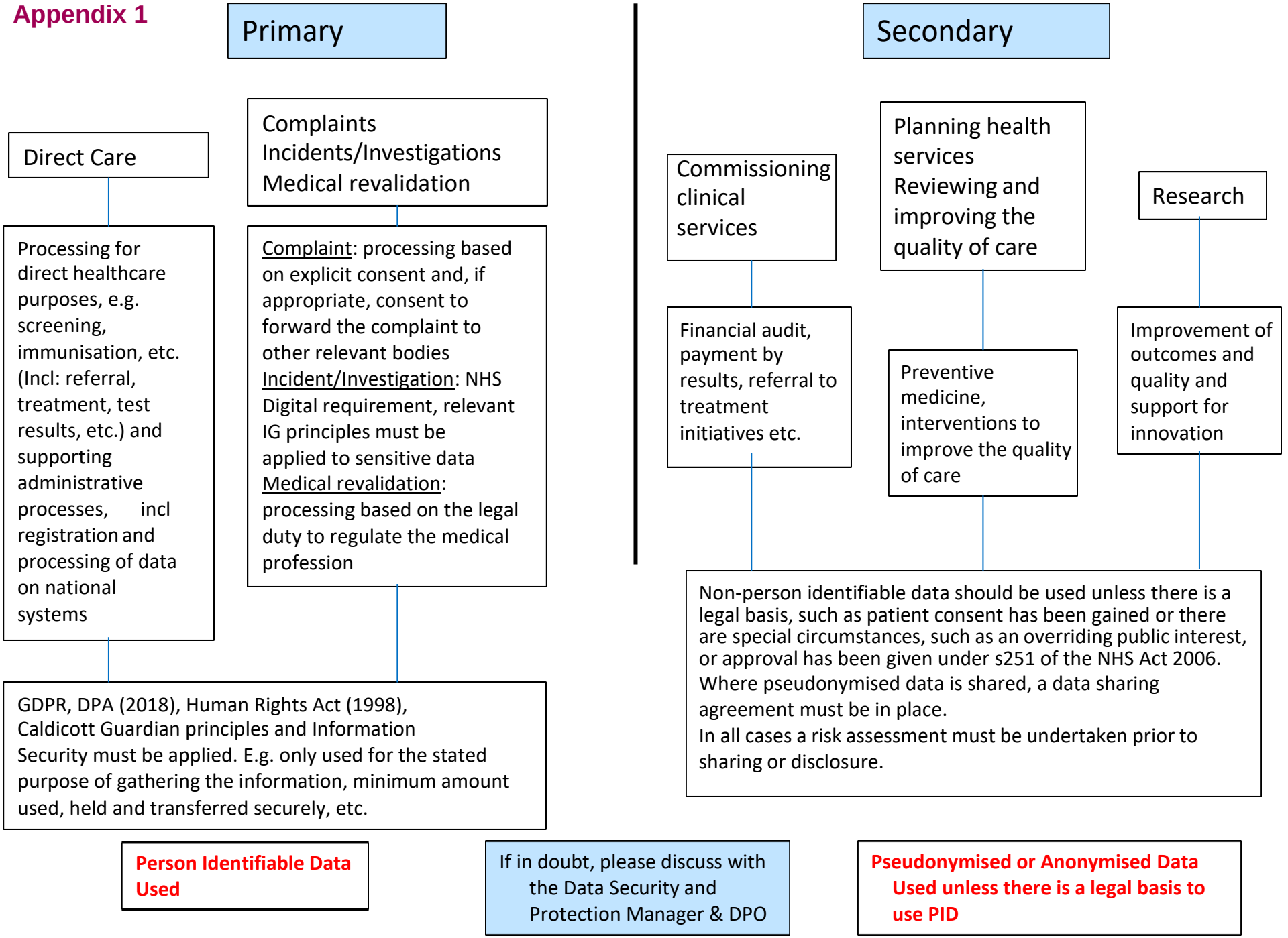
- Managers and Directors – to disseminate within their areas
- Staff - via newsletter
- Published to the Trust intranet via its daily digest newsletter
- Awareness raising by Senior Managers

10 References and resources

ISO/TS 25237:2008 - Health Informatics Pseudonymisation Standards -	Provides details of the minimum standards for the operation of a pseudonymisation service. Available to purchase from the British Standards Institute website.
General Social Care Council: Code of Practice for Social Care Workers & Employers	These codes of practice set out standards of practice and conduct for social care workers and their employers. Registrants with the General Social Care Council are required to comply with the codes as a condition of ongoing registration.
DH: Confidentiality NHS Code of Practice 2003	The Code is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to use their information.
DH: The Caldicott Guardian Manual 2010	The Manual is guidance that takes account of developments in information management in the NHS and in Councils with Social Services Responsibilities since the publication of the Caldicott report 1997. It sets out the role of the Caldicott Guardian within an organisational Caldicott/confidentiality function as a part of broader information governance.
The NHS Care Record Guarantee for England	The Guarantee sets out the rules that govern how patient information is used by all organisations providing care for or on behalf of the NHS and what control the patient can have over this.

DH: Informatics Planning 2010/2011 (PDF, 913 KB)	This Informatics Planning guidance is published alongside the NHS Operating Framework for 2010/11, to provide detailed guidance regarding the informatics elements of local operating plans.
Anonymisation Code	Summary of the Anonymisation Code of Practice
Anonymisation Standard	The Anonymisation Standard for Publishing Health and Social Care Data.
Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013 (PDF, 373 KB)	BSI UK document showing the mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013.
Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013 (PDF, 497 KB)	BSI UK document designed to help meet the requirements of the new international standard for information security management, ISO/IEC 27001:2013, which is the first revision of ISO/IEC 27001:2005.
UK Anonymisation Network - useful website	The UK Anonymisation Network (UKAN) has been set up as a means of establishing best practice in anonymisation and offers practical advice and information to anyone who handles personal data and needs to share it.

Appendix 1


Primary
Secondary
Direct Care
Complaints
Incidents/Investigations
Medical revalidation
Commissioning clinical services
Planning health services
Reviewing and improving the quality of care
Research
Processing for direct healthcare purposes, e.g. screening, immunisation, etc. (Incl: referral, treatment, test results, etc.) and supporting administrative processes, incl registration and processing of data on national systems
Complaint: processing based on explicit consent and, if appropriate, consent to forward the complaint to other relevant bodies
Incident/Investigation: NHS Digital requirement, relevant IG principles must be applied to sensitive data
Medical revalidation: processing based on the legal duty to regulate the medical profession
Financial audit, payment by results, referral to treatment initiatives etc.
Preventive medicine, interventions to improve the quality of care
Improvement of outcomes and quality and support for innovation
Non-person identifiable data should be used unless there is a legal basis, such as patient consent has been gained or there are special circumstances, such as an overriding public interest, or approval has been given under s251 of the NHS Act 2006.
Where pseudonymised data is shared, a data sharing agreement must be in place.
In all cases a risk assessment must be undertaken prior to sharing or disclosure.
GDPR, DPA (2018), Human Rights Act (1998), Caldicott Guardian principles and Information Security must be applied. E.g. only used for the stated purpose of gathering the information, minimum amount used, held and transferred securely, etc.
Person Identifiable Data Used
If in doubt, please discuss with the Data Security and Protection Manager & DPO
Pseudonymised or Anonymised Data Used unless there is a legal basis to use PID