Essex Partnership University
NHS Foundation Trust

# PSEUDONYMISATION PROCEDURE

| | |
|---|---|
| **POLICY REFERENCE NUMBER** | CPG72 |
| **VERSION NUMBER** | 2 |
| **KEY CHANGES FROM PREVIOUS VERSION** | 3 year review. New section 3.2 added; new section 4.1.5; s5.1 amended; amendments in s8.1.1; deletion of s8.1.2 |
| **AUTHOR** | Business Analysis and Reporting Manager<br>Head of Information & Performance |
| **CONSULTATION GROUPS** | Information Governance Steering Group<br>Information Teams |
| **IMPLEMENTATION DATE** | May 2018 |
| **AMENDMENT DATE(S)** | September 2021 |
| **LAST REVIEW DATE** | September 2021 |
| **NEXT REVIEW DATE** | September 2024 |
| **APPROVAL BY IGSSC** | August 2021 |
| **RATIFICATION BY QUALITY COMMITTEE** | September 2021 |
| **COPYRIGHT** |  |

**PROCEDURE SUMMARY**

The implementation of this procedural document will ensure that all staff working within Essex Partnership University NHS Foundation Trust (EPUT) understand the importance of, and how to pseudonymise patient identifiable information, and are able to provide assurance to the Trust that the security of patient identifiable information to be transferred has been properly considered.

**The Trust monitors the implementation of and compliance with this policy in the following ways:**

The Information Governance Steering Group will have overall responsibility for overseeing the implementation of this procedure. The Trust will continue to work towards compliance to information governance and data protection. The policy and procedure will be reviewed every three years in line with Trust policy or when legislation, national or local guidance requires.

| Services | Applicable | Comments |
|---|---|---|
| Trustwide | ✓ | |
| Essex MH & LD | ✓ | |
| CHS | ✓ | |

**The Director responsible for monitoring and reviewing this procedure is Executive Chief Finance Officer**

**EPUT**

# PSEUDONYMISATION PROCEDURE

**ASSURANCE STATEMENT**

The implementation of this procedure will ensure that all staff working within Essex Partnership University NHS Foundation Trust (EPUT) understand the importance of, and how to pseudonymise patient identifiable information, and are able to provide assurance to the Trust that the security of patient identifiable information to be transferred has been properly considered.

## 1.0 BACKGROUND

1.1 A fundamental principle of the *Data Protection Regulation (GDPR)* 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.

## 2.0 INTRODUCTION

2.1 Pseudonymisation is a method which allows organisations to disguise the identity of patients by creating a pseudonym for each patient identifiable data item, allowing patient linking analysis / referencing for secondary uses.

2.2 Pseudonymisation is a core element of Secondary Uses Services (SUS), and should be applied across the Trust.

2.3 Pseudonymisation should be applied to data held within secure databases.

## 3.0 PURPOSE

3.1 In order to protect patient identifiable information staff must only have access to the data it is necessary for them to have to complete the business activity which they are involved in.

3.2 The purpose of this document is to provide guidance for staff so that Patient Identifiable Data (PID) is processed legally and securely, and to ensure that staff understand when and how data should be pseudonymised or anonymised.

3.3 This applies to the use of person identifiable data (PID) for secondary or non-direct healthcare purposes.

3.4 The pseudonymisation of information / data allows users to use patient data for a range of secondary purposes without having to access the identifiable data items.

## 4.0 DEFINITIONS

### 4.1 Definitions

#### 4.1.1 Person Identifiable Data (PID)

Any information that can identify an individual – this could be one piece of data, e.g. a persons' name or a collection of data, e.g. address and date of birth.

#### 4.1.2 Primary Use

When information is used for healthcare and medical purposes and directly contributes to the treatment, diagnosis or the care of an individual, including relevant supporting administrative processes and audit / assurance of the quality of healthcare provided.

#### 4.1.3 Secondary Use

For non-healthcare and medical purposes, e.g. research purposes, audits, service management, commissioning, contract monitoring and reporting facilities. When PID is used for secondary use this should be limited and pseudonymised so that the secondary use process is confidential.

#### 4.1.4 Pseudonym

A name that a person or group assumes for a particular purpose, which can differ from their original or true name to conceal identity

#### 4.1.5 Pseudonymised Data

Pseudonymised (or key-coded) data is where a unique identifier is used to disguise the personal identity of a person

## 5.0 BUSINESS REQUIREMENTS

5.1 Business requirements for primary use is for the sharing of raw data outside of the Trust.

5.2 Business processes for secondary use must be undertaken with unidentifiable data and any processes using PID must be modified in line with these procedures. By de-identifying data, users are able to make use of patient data for a range of secondary purposes without having access to the identifiable data items.

5.3 Where a business process requires confirmation of a patient (e.g. that a patient is registered with a GP) this area can be identified via the safe haven route (section 8.2)

5.4 Systems must be put in place to ensure that staff only have access to information they require for business activity they are involved in, as identified under the Caldicott principles ('*access should be on a need to know basis*')

5.5 Even when pseudonymised, data items should still be used within a secure environment with staff access strictly controlled /authorised on a 'need to know' basis. This can be achieved by:

5.5.1 Pseudonymisation techniques can be consistently applied. The same pseudonym can be provided for individual patients across different data sets, to allow the linking / referencing of data sets and other information which is not available if the PID is removed completely.

5.5.2 Where patient data is required the NHS Number is the most secure form of identifiable data and should be used.

## 6.0 LOCAL PATIENT IDENTIFIER

### 6.1 Local Patient Identifier

Within the Trust, the use of patient identifiable information is restricted to the use of the 'local patient identifier', which is recorded within the patient information system. This eliminates the need to include identifiable information such as the forename, surname, Date of Birth (DoB), gender, ethnicity etc.

*A breakdown of information by identifiers such as ethnicity and gender is permitted, providing the number per group is not less than 7. Numbers smaller than this can potentially lead to the discovery of an individual's identity; therefore this information will be supressed and notified to the recipient as being supressed.*

Where information is to be sent externally, there will be a secondary unique identifier created, such as a new reference number, either for each patient or for each event, and used consistently. The patient identifiers, such as forename and surname, are removed before submission to ensure patient confidentiality. This allows the external agencies/organisations to interrogate this information by referring to the secondary identifier i.e. a new reference number.

### 6.2 Identifiable patient information

There are certain circumstances where it has been agreed that identifiable information, other than just the local patient identifier, can be shared. The following table gives the organisations with which the Trust shares identifiable data for non-patient care purposes.

| Organisation | NHS Digital | Commissioners | Essex County Council | National Drug and Treatment Systems |
|---|---|---|---|---|
| Type of organisation | NHS | NHS | Social Services | Social Services |
| Type of person identifiable information | All identifiable information of all service users, unless consent has been refused | Name, NHS Number, Gender and Year of birth for appropriate patients | Names and date of birth for those who are entitled to S117 after care | All identifiable information of all service users receiving substance misuse treatment, unless consent has been refused |

| | | | | |
|---|---|---|---|---|
| Purpose for sharing | Minimum Dataset | To enable validation of cost and volume invoices | To ensure responsibility for section 117 aftercare is appropriately provided | Minimum Dataset |
| Transmission method | Secure electronic portal | Secure electronic portal | Password protected document to secure email address | Secure electronic portal |

## 7.0 PSEUDONYMISATION OF DATA

### 7.1 Pseudonymisation of Data

7.1.1 To effectively pseudonymise data the following actions / steps must be taken:

- Each field of PID should have a unique pseudonym
- Pseudonyms are to be used in place of identifiable data such as NHS numbers. The Pseudonym should be of the same length / format as the original data to ensure readability (e.g. pseudonym for NHS Number should read 123 123 1230) – the use of letters and numbers should be considered to avoid confusion with original data.
- Consideration must be given to the potential impact on existing systems
- Pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised
- Secondary use output must only display the pseudonymised data items that are required in accordance with Caldicott guidance
- Pseudonymised data should have the same security applied to it as identifiable data

### 7.2 Use of Identifiable Data

7.2.1 If PID data is required, the reasons and usage for the data should be fully documented and approval sought by the data owner.

7.2.2 The auditable trail of access to patient records supports the Care Record Guarantee where patients are to be informed as to who has accessed / seen their data. The audit will provide accurate data in the event of untoward incidents. Key items to be documented will be:

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

7.2.3 The log of access should be regularly audited via sampling of users or subject matter to check for unusual patterns of access and these should be reported to the Information Governance Team.

### 7.3 Transferring of Data

7.3.1 Appropriate data sharing agreements, in line with Trust policy, should be in place when information is to be transferred to another organisation

## 8.0 PROCESSES FOR PSEUDONYMISATION

### 8.1 Encryption

#### 8.1.1 Encrypted information

In instances where the DOB, NHS number, postcode or patient name must be included, encryption of these items will be used.

For all other occasions when this encryption would be required, the approval of the Caldecott Guardian is required.

Examples of encryption are:

**DOB** (dependent on the encryption key)
Date of birth could be transferred into age range

**NHS number** (dependent on the encryption key)
NHS number could be doubled

**Postcode or name** (dependent on the encryption key)
Postcodes could be shortened to first half of postcode
Names could become an anagram

The encrypted information is passed to the external organisation via a secure email address on a password protected document.

#### 8.1.2 Encryption Use Log

Below is an example of a log that can be kept for instances of encryption being required:

| Date of request | Name of organisation | Purpose | Date of approval by the Caldicott Guardian | Type of pseudonymisation |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

### 8.2 Safe Haven

8.2.1 The NHS has used safe haven practices for over 20 years for the secure transfer of person identifiable information / data. The Trust procedure (CPG50C) provides safe haven guidance in relation to transferring information via fax, post, telephone, etc. For the purpose of pseudonymisation the safe haven procedures below must be observed.

8.2.2 All PID must be stored within a new safe haven environment to which only limited and authorised staff have access to.

8.2.3 The concept of the safe haven principles, in relation to pseudonymisation, is that of restricting access to identifiable data which is required to support the process of de-identifying records.

8.2.4 Patient information systems and databases must be within an electronic safe haven whereby access is limited and password controlled for each authorised user.

8.2.5 Access to new safe havens will be given by the Trust's IT&T Department, based on manager authorisation.

8.2.6 A register of authorised new safe haven environment users will be maintained for each database / system by the Information Asset Owner and a full list maintained by the Information Governance team.

## 9.0 DATA SECURITY & PROTECTION TOOLKIT

### 9.1 Links to the Data Security & Protection Toolkit (DS&P Toolkit)

9.1.1 The Trust must identify all flows of person identifiable data, both internal and external, reporting any identified risks and associated action planning in line with the DS&P Toolkit requirements.

9.1.2 The Trust must register who has access to the identifiable data, the reasons for the access and what they do with the data / information.

9.1.3 Where appropriate the Trust must ensure that access to identifiable data is achieved by the use of a Smart Card, in line with national guidance on the use of Smart Cards.

9.1.4 End user applications / reports that provide patient level data must be modified to enable separate views of pseudonymised and identifiable data.

9.1.5 Audit logs / trails should be maintained and access to systems monitored and reported to the Information Governance Steering Group to ensure that the correct staff are accessing the PID and that this is being accessed for limited purposes.

## 10.0 TRAINING

10.1 Appropriate training on the implementation and use of pseudonymised information / data will be provided by the Trust's Information Departments as required.

10.2 General training for information governance / security will be undertaken by all staff in line with mandatory, national requirements.

**END**