Essex Partnership University
NHS Foundation Trust

# PSEUDONYMISATION POLICY

| | |
|---|---|
| **POLICY REFERENCE NUMBER** | CP72 |
| **VERSION NUMBER** | 2 |
| **KEY CHANGES FROM PREVIOUS VERSION** | 3 year review; s1.1 – DPA added; new section 2.2; s3.2 – additional sentence at end; s6.1 – updated with new links and content |
| **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** |  |

**POLICY SUMMARY**

The implementation of this policy and its associated 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.

**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 policy and its associated 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 policy is Executive Chief Finance Officer**

**EPUT**

# PSEUDONYMISATION POLICY

**ASSURANCE STATEMENT**

The implementation of this policy and its associated 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 INTRODUCTION

1.1 The EU General Data Protection Regulation (GDPR), the Human Rights Act 1998, the Data Protection Act (DPA) 2018 and the common law relating to duty of confidentiality apply to all NHS organisations and require that the minimum personal data are used to satisfy any particular purpose, 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.

1.2 Planning guidance published by the Department of Health in support of the 2010/11 Operating Framework sets clear targets for NHS bodies, stating that:

"It is NHS policy and a legal requirement that patient level data should not contain identifiers when they are used for purposes other than the direct care of patients, including local flows between organisations as well as data extracted from the *Secondary Uses Service*".

## 2.0 AIMS & OBJECTIVES

2.1 The key principle / aim is to ensure, as most practical and reasonable, that individual patients cannot be identified from data that is used to support purposes other than their direct care or to quality assure the care provided.

2.2 The implementation of this policy & procedure will support compliance with legislation and best practice

2.3 Where it is not practical or reasonable to pseudonymise data EPUT will ensure that data will be processed in a way that minimises the risk to that data.

2.4 This policy and associated procedure also aims to identify different levels or personal information anonymisation, identify different types of organisations information is shared with and consider different anonymisation methods.

## 3.0 WHAT IS PSEUDONYMISATION AND ANONYMISATION

3.1 Pseudonymisation and Anonymisation are methods that disguise the identity of patients by creating a pseudonym for patient identifiable data items.

3.2 Pseudonymisation is an overarching term for procedures that strip identifiable information from personal data. It is used to protect privacy and enables organisations to minimise the impact of a data breach. Pseudonymisation methods are outlined in the associated procedure.

3.3 The aim of pseudonymisation is to obscure identifiable data items within the patient records sufficiently so that the risk of possible identification of the subject is minimised to acceptable levels. A typical Pseudonymisation will replace the NHS number with an alternative unique number.

3.4 Anonymisation is a process whereby data is turned into a form which does not contain any identifiable information to allow a wider use of the information.

3.5 Pseudonymisation and anonymisation are both processes that strip identifiable information however Pseudonymisation typically involves a reversible process whereas anonymisation is irreversible.

## 4.0 SCOPE

4.1 This policy and associated procedure applies to all EPUT staff and must be used by all staff involved in the use / dissemination of secondary / other non - direct healthcare patient information / data.

4.2 This policy and associated procedure applies to any information transferred to another organisation that includes patient identifiable data or that may impact on the privacy of individuals

## 5.0 ROLES AND RESPONSIBILITIES

### 5.1 Chief Executive

The Chief Executive has overall responsibility within the Trust, as accountable officer, for the appropriate information security measures required to protect person identifiable information / data.

### 5.2 Associate Director of Business Analysis and Reporting

The Associate Director of Business Analysis and Reporting will be responsible for ensuring appropriate measures are developed, implemented, followed and enforced to ensure Pseudonymisation of secondary care / other (not directly used for patient healthcare) information / data underpins the work of the Trust.

### 5.3 Caldicott Guardian

The Caldicott Guardian has responsibility for ensuring that patient information is shared in an appropriate and secure manner that protects patient's privacy and interests.

**5.4 Individuals**

All staff working for the Trust are responsible for ensuring that all information /data used is pseudonymised wherever the patient identifiers are not required for the purpose of the use of the information /data.

**5.5 Information Governance Steering Committee**

The Committee will be responsible for overseeing the information governance / security aspects of the implementation and on-going practice of pseudonymising information / data.

## 6.0 RELEVANT LEGISLATION AND GUIDANCE

6.1 This policy and its associated procedural guidelines have been developed in line with national / local guidance from:

- General Data Protection Regulation
- Data Privacy Impact Assessments
- Data Security & Protection Toolkit
- Caldicott Principles
- Confidentiality: NHS Code of Conduct
- Data Protection Act 2018

## 7.0 REFERENCE OTHER TRUST DOCUMENTS

Other related Trust policies and procedures may be read in conjunction with this policy:

- Information Governance / Security Policy and Procedures
- Safe Haven Procedure
- Records Management Policy and Procedures
- Registration Authority Policy and Procedures

## 8.0 MONITORING AND REVIEW

8.1 The Information Governance Steering Group will have overall responsibility for overseeing the implementation of this policy and its associated procedural guidelines, taking forward any action relating to information governance / security within the Trust.

8.2 The Director of ITT, Business Analysis and Reporting is the specific senior manager responsible for co-ordinating, publicising and monitoring implementation of this policy and its associated procedural guidelines.

8.3 This policy and its associated procedural guidelines will be reviewed every three years in line with Trust policy or when legislation, national or local guidance requires.

8.4 The Trust will work towards full and continued compliance to information security management systems, ensuring independent audits are undertaken, as appropriate or dictated by guidance.

**END**