Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: IM4
Issue number: 5

Standards of secondary use of information policy

Lead executive	Director of Finance
Authors details	Associate Director of Performance & Redesign 01244 393304

Type of document	Policy
Target audience	All CWP staff
Document purpose	To provide guidance on the management of access to identifiable data.

Approving meeting	Information Governance & Data Protection Sub-Committee	13/03/2019
Implementation date	September 2019	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy Trust Data Quality Framework

Document change history	
What is different?	Change of job title in section 5, from Head Of Performance & Information to Head of Business Intelligence & Management Information.
Appendices / electronic forms	N/A
What is the impact of change?	N/A

Training requirements	No - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	N/A

Financial resource implications	None

External references
1. N/A

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
N/A		
Is the impact of the document likely to be negative?	No	
- If so can the impact be avoided?	N/A	
- What alternatives are there to achieving the document without the impact?	N/A	
- Can we reduce the impact by taking different action?	N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	N/A	
What is the level of impact?	N/A	

Contents

1. Policy for Pseudonymisation

This sets out the policy of Cheshire & Wirral Partnership NHS Foundation Trust in respect of achieving and maintaining the principles of pseudonymisation in so far as it relates to the management and use of identifiable data within the Trust.

2. Policy objectives

The objectives of this policy are as follows:

- To ensure that, where possible, routine use of data should employ de-identified data;
- To ensure that the identifiable data that is used within the organisation is maintained and managed in a confidential manner;
- To ensure that there are proper and duly authorised processes in place to control access by staff to the identified data;
- To ensure there are appropriate processes in place for the acquisition and retention of identifiable data;
- To ensure that appropriate governance arrangements exist for the management of this policy;
- To ensure there are proper processes in place for the issue of de–identified data for wider use;
- To ensure the existence of appropriate skills, knowledge and techniques in relation to Pseudonymisation and for the construction and issue of de-identified data sets.

3. Policy detail

3.1 Safe Haven

Identifiable data used by the Trust will be maintained within a 'safe haven' environment. The characteristics of this 'safe haven' will be:

- Only a limited set of staff of the Trust will be authorised to have access to and work with the identifiable data held within it;
- Staff granted access to work within the 'safe haven' must be approved by departmental management and a safe haven management body;
- Data used outside of the safe haven must be de-identified before issue;
- Data flows, both inbound and outbound to and from other organisations will only take place using the safe haven, encryption email or nhs.net account when identifiable data is to be exchanged;
- Identifiable data will therefore only exist and be manipulated within the safe haven by a limited number of duly authorised staff. Any data issued outside of the safe haven for secondary use will consequently be either aggregated tables or de identified individual records. The process of de-identification will require the following:
  - Removal of any name and address fields;
  - Conversion of data of birth to age in years at time of event, immediate implementation;
  - Removal of NHS number and replacement with a system record ID, immediate implementation;
  - Conversion of post code to LSOA code this element will be reviewed within the compliance plan to meet IG Level 2 standards.

3.2 External data flows

In bound and outbound flows of identifiable data will take place ensuring that the data transfer is secure by means of nhs.net email account, encryption email or direct link safe haven to safe haven.

4. Issue of de-identified data for secondary use within the Trust

Data for secondary use within the Trust may be issued from the safe haven as described above. A record will be kept of which de-identified data has been issued and reason(s) the access has been granted.

5. Governance arrangements for the policy

The policy will be managed by the Head of Business Intelligence and Management Information, delegated from the Associate Director of Performance and Redesign. The remit of the policy control will be:

- To review and monitor the operation of the policy.

To review, monitor and implement guidance to manage the access control for the safe haven, report manager and identifiable data requests. To work with management colleagues, in particular the Data Warehouse Team, the Clinical Systems Manager and service delivery managers, to implement policy.

To review and monitor the data defined as falling within the remit of this policy. Where necessary, consultation on specific matters will take place with the following:

- Associate Director of Performance and Redesign.

6. Access to the safe haven data

Staff will only be granted access to the safe haven where there is a clear 'need to know' in the context of the job the member of staff is employed to do. The intention is that only a limited number of staff will meet the 'need to know' criterion.

This refers to DBA staff having full access to the raw data sources within the Data Warehouse, and the limited access the Performance and Information team have to the defined datasets, for reporting.

All staff with access to safe haven data will be required to ensure they treat access to the data with attention to the requirements of data confidentiality and security.