Mid Essex Hospital Services NHS
NHS Trust

New Safe Haven	**Policy** **Register No: 12001** **Status: Public once ratified**

Developed in response to:	Best Practice Information Governance Toolkit
Contributes to CQC Outcome	

Consulted With	**Post/Committee/Group**	**Date**
Bhavesh Khetia	Information Governance Manager	March 2016
Caroline Holmes	Head of Clinical Coding and Data Quality	March 2016
Professionally Approved by	Martin Callingham, Chief Information Officer	March 2016

Version Number	2.0
Issuing Directorate	Informatics
Ratified by:	DRAG Chairmans Action
Ratified on:	21st March 2016
Executive Management Group Sign Off Date	April 2016
Implementation Date	22nd March 2016
Next Review Date	February 2019
Author/Contact for Information	Ian Harrison, Head of Information Services
Policy to be followed by (target staff)	Authorised Staff within Information Services
Distribution Method	Intranet, Trust website
Related Trust Policies (to be read in conjunction with)	Serious Incident Requiring Investigation policy Information Security Management Strategy Confidentiality Policy Data Protection Policy Sharing Patient Information Policy Email Policy Sending Patient Identifiable out of the UK Information Governance Handbook Sharing Patient Identifiable Data

Document Review History

Version No	**Authored/Reviewed by**	**Active Date**
1.0	Ian Harrison, Head of Information Services	1 February 2012
2.0	Ian Harrison, Head of Information Services	21 March 2016

Index

1.0 Purpose

1.1 The purpose of this policy is to document the Trust's new safe haven arrangements and to define exclusions to the policy.

2.0 Background

2.1 The NHS has used Safe Havens for a number of years to ensure the safety and secure transfer of Person Identifiable Data (PID). The primary use has been to provide security when fax machines have been used to transmit patient data between organisations. The Trust's Information Governance Handbook section 3.4 contains guidance on the best practice for this activity.

2.2 'New Safe Haven' (NSH) is the term used to cover the restriction of access to Person Identifiable Data for a secondary use (i.e. not directly linked to patient care).

2.3 This restriction should allow access by a numerically small group of authorised staff sufficient to undertake the specific functions. The NSH can be defined in terms of access control and data management arrangements or by the functions and the related system activities.

3.0 Scope of Policy

3.1 The Data Protection Act 1998, the Human Rights Act 1998 and the common law relating to confidentiality apply to all organisations. They 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), and that information obtained in confidence should not normally be used in an identifiable form without the permission of the individual it relates to.

3.2 Planning guidance published by the Department of Health in support of the annual Operating Framework sets clear targets for NHS bodies. It states that:

It is NHS Procedure 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.

3.3 All NHS Commissioners and providers of NHS commissioned care should:

- ensure that relevant staff are aware of and trained to use de-identified data
- ensure appropriate changes are made to processes, systems and security mechanisms in order to facilitate the use of de-identified data in place of patient identifiable data
- use the latest IG Toolkit to assist in implementation and assessment of compliance with Procedure and legal requirements

3.4 The key principle is to ensure, as far as is practicable, that individual patients 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 de-identified data.

3.5 The Trust's NSH' will provide the means of restricting access to identifiable data to authorised users, specifically for the purposes of receiving and sending identifiable data that is to be used for a secondary use.

3.6 The NSH can be defined in terms of

- the activities to be undertaken to support de-identification
- posts/people authorised to access identifiable data for the purpose of supporting de-identification
- posts/people authorised to access identifiable data for the purpose of supplying identifiable data to authorised users
- the facilities necessary to support the activities

3.7 The intention of the NSH is that it will ensure that:

- the facilities can only be used by a small number of authorised staff
- authorisation of those staff is closely controlled
- there is restricted access to the systems used to generate the data used for secondary use
- the Trust conforms to NHS good practice concerning the handling of identifiable data (as predicated by ISO 27001 and 27002 and the CFH Good Practice Guidance)

4.0 Responsibilities

4.1 **Chief Executive** - overall responsibility for the New Safe Haven Policy

4.2 **Senior Information Risk Officer (SIRO)** – delegated responsibility for the day-to-day operation of the policy. The SIRO chairs the Information Governance Group (IGG).

4.3 **All staff with responsibilities to provide clear or de-identified data internally or externally to the Trust** must comply with this policy. Any non-compliance will be considered a breach which will be reported as a Trust Incident.

5.0 New Safe Haven – Overriding Principles

5.1 For the avoidance of doubt, the new safe haven arrangements will not apply where the data exchange is for purposes that directly contribute to the safe care of a patient, and include care, diagnosis, referral and treatment processes together with relevant supporting administrative processes (a Primary Purpose).

5.2 The NSH for the Trust will only consist of the staff within the Information Services Department. This Department reports to the Director of Business Development and Performance.

5.3 Information Services staff will use the Data Warehouse as the primary source of patient activity based information. Access to this system is limited by the install of agent software on specific PC hardware or via a secure SQL link and staff

being member of a specific login group, managed centrally by the IT Department.

5.4 Trust staff will only use NHS.Net email accounts or the secure shared drive with NHS Mid Essex to share Person Identifiable Data with other organisations.

5.5 Data will be de-identified using the methods described in the 'Sharing Patient Level Data Policy.

6.0 Exclusions from New Safe Haven Arrangements

6.1 The following transfers of data are excluded from the new safe haven arrangements:

- Commissioning Data Set (CDS) files sent to the NHS Secondary Uses Service (SUS). These are generated from the PAS application
- Contracted and specifically requested data transfers to commissioners including NHS Mid Essex CCG
- Out of Area Treatment cost recovery data transfers to other CCGs
- NHS required data transfers using the UNIFY2 service
- Data transfers made in support of Section 251 excluded studies, as determined by the National Information Governance Board (NIGB)
- Data transfers made where a Data Processing Agreement or Data Sharing Agreement have been signed by both parties
- Data transfers made to the 'New Safe Haven' area of other NHS and non-NHS organisations, where this is carried out using secure means (NHS.Net email or file encryption)
- Data transfers made to NHS national web based applications (e.g. NN4B, PDS)

7.0 Inter-Organisational Data Transfers

7.1 Where a data transfer between organisations is for a secondary use the data must be de-identified in line with the Trust 'Sharing Patient Identifiable Data' policy.

7.2 Where a data transfer is between NSHs or the Trust NSH and a service supporting direct care, then it is appropriate to use identifiable data, such as NHS number and data of birth as patient labels if they are available.

8.0 Breaches of the Policy

8.1 All perceived breaches must be reported to the Trust Information Governance Manager or SIRO so that a judgement can be made as to whether the incident constitutes a "Serious Incident" to be investigated under the Serious Incident Requiring Investigation policy.

8.2 Outcomes of all investigations will be reported at the IGG.

9.0 Monitoring and Audit

9.1 An annual audit based on a sample of data leaving the NSH will be taken and the results reported to the Senior Management Team Meeting.

10.0 Communication and Implementation

10.1 The Information Governance team will upload the policy to the intranet and website and notify staff via the Staff Focus

10.2 Information Services Staff will be sent a personal copy by e-mail and the policy will be discussed at the first monthly team meeting following approval

10.3 New Information Services staff will be given a copy at their local induction

11.0 References

Information Governance Toolkit