New Safe Haven Policy

Department / Service:	Corporate Policy
Originator:	Information Governance Manager
Accountable Director:	Chief Finance Officer
Approved by:	Information Governance Steering Group Trust Management Executive
Date of approval:	10th June 2019
First Revision Due:	10th December 2020
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All
Target staff categories	All

Policy Overview:
The purpose of this policy is to ensure that staff at Worcestershire Acute NHS Hospitals Trust has access to guidance around secure methods of transferring and communicating personal identifiable data and the requirements for Safe Havens. As part of the section on Safe Haven procedure, the policy sets out Department of Health Policy on the requirements to only use identifiable data for primary care purposes and to anonymise or pseudonymise identifiable data when it is used for secondary or "business" purposes, where practicable.

Latest Amendments to this policy:
Minor update including, relevant dates and approval Appendices removed and available on the Information Governance Webpages 12th June 2020 – Document extended for 6 months whilst in order to have the resource to update and consider any local or national changes to be incorporated.

Contents page:

Appendices

None

Supporting Documents

Supporting Document 1 Equality Impact Assessment
Supporting Document 2 Financial Risk Assessment

Quick Reference Guide – Safe Haven Policy

NHS Safe Haven's

All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of the personal information. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive information (e.g. patient information).

Definition of a Safe Haven within this policy

A location (or system) within an organisation where arrangements and procedures are in place to ensure personal information can be stored, received and communicated securely.

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 pseudonymised or anonymised data

Legislation and Guidance

Information on the Caldicott Principle and the Data Protection Act 1998

Below is a brief overview of the areas included within the Safe Haven Policy

Old Safe Haven Processes

- Guidance on security arrangements for 'Safe Havens' within the organisation
- Guidance on Faxing person identifiable data, to and from the organisation
- Guidance on posting person identifiable data, to and from the organisation
- Guidance on electronically sending person identifiable data, to and from the organisation
- Breaches of confidentiality – reporting within the Trust

New Safe Haven Processes

- Guidance on the principles that apply to patient level data for secondary and non-direct care purposes and if pseudonymisation and anonymisation is needed
- Guidance on the utilisation of de-identification tools enables users to make use of patient level data for a range of secondary purposes without having to access those data items, which may reveal the identity of the patient.
- Guidance on distinguishing between Primary and Secondary staff to ensure that the personal data that they have access to is correct to their role

1. Introduction

All NHS organisations require safe haven procedures to maintain the privacy and confidentiality of the personal information. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive information (e.g. patient information).

2. Scope of this document

This policy provides:

- The legislation and guidance which dictates the need for a safe haven
- When a safe haven is required
- The necessary procedures and requirements that are needed to implement a Safe Haven
- Rules for different kinds of safe haven
- Who can have access to information

3. Definitions

Safe Haven	A location (or system) within an organisation where arrangements and procedures are in place to ensure personal information can be stored, received and communicated securely. 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 pseudonymised or anonymised data
Pseudonymised	Pseudonymisation is a method of anonymising patient level data which provides the same pseudonym to individual patients across different data sets and over time. This allows for linking of patient events without being able to identify the patient, whereas fully anonymised data cannot be linked. De-Pseudonymisation is where the identifiable information is put back into the patient's data so it can be used for patient care again
Anonymised	Data that has been permanently stripped of all personal identifiers
Personal Information	Personal information is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name and address, name and home telephone number, etc.
Sensitive Personal Information	Sensitive personal information is where the personal information contains details of that person's: • Health or physical condition • Sexual orientation • Ethnic origin • Religious beliefs • Political views • Criminal convictions
PCD	**Person Confidential Data** This is information/data about a person which would enable that person's identity to be established by one means or another. Name and address are very strong identifiers, particularly when available together.

4. Responsibility and Duties

Information Governance Steering Group
The Information Governance Steering Group (IGSG) is responsible for providing policies and guidance to ensure staff share information in a secure manner to maintain patient confidentiality at all times.

Information Governance Manager
The Information Governance Manager will work with departmental managers to ensure that any data that is transferred from departments will be assessed for risks (Data Mapped) and staff will be advised on confidentiality and safe haven principles. Data mapping results will be loaded into the Information Governance Toolkit Data Mapping Tool and the results will be reported to the IGSG/SIRO. Departments where PCD is transferred on a regular basis will follow the same process.

Data Transfer incidents will be monitored along with all other Information Governance incidents and reported to the IGSG/SIRO.

Information Department
The Information team are responsible for assessing requests for patient information and using anonymisation or pseudonymisation processes where appropriate.

The Caldicott Guardian
The Caldicott Guardian is responsible for authorising requests for patient information by secondary users.

All Acute Trust Staff
All staff have a responsibly to comply with this policy and ensure that any information is shared appropriately and lawfully. All staff must complete their annual IG training to ensure that they are aware of their responsibilities regarding viewing and sharing information.

5. Safe Haven Processes

Old Safe Haven Principles: Appendix 2 sets out best practice for transporting PCD via fax and email

Pseudonymisation and Anonymisation (New Safe Haven)

There is an overarching Information Governance principle that users should only have access to data that are necessary for the completion of the business activity which they are involved in. This is reflected in Caldicott Principles 1, 2 and 3. These principles apply to the use of patient level data for secondary or non-direct care purposes. The utilisation of de-identification tools enables users to make use of patient level data for a range of secondary purposes without having to access those data items, which may reveal the identity of the patient. See the Pseudonymisation Policy for specific details on anonymisation standards

It is necessary to distinguish between the two types of use in order to determine what data a user can see. Examples of secondary use of patient data are performance management, commissioning, contract monitoring; all of which do not require the identity of patients. There are functions within the NHS that use the same data sources for both secondary and primary uses. An example at CCG level would be for performance monitoring of Referral to Treatment (RTT) which should use de-

identified data, but for organising care provision within 18 weeks, access to identifiable data is a primary use and therefore permissible by a suitably authorised member of staff.

The key principle is to ensure, as far as is practicable, that individual service users cannot be identified from data that is 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 pseudonymised or anonymised data. The Trusts information department has a process in place to provide this function.

For the purpose of safe havens, the trust has separated staff into either Primary or Secondary users:

Primary Staff:
This group includes system users working for the following types of departments and dealing with personal data – they would routinely see personal data:

- Clinical and support staff
- Health Records
- Medical Secretaries
- Information
- Complaints
- Directorate Management

Secondary Staff:
This group of staff would not routinely see personal data and any data that they required should be anonymised:

- Domestic staff
- Supplies
- Estates
- Procurement
- Human Resources (patient's information)
- Porters/Post Rooms
- Consulting Firms – Data Analysis
- Service Reviews
- Financial Services

Caldicott Approval
Where PCD information has to be shared outside of the primary group, Caldicott approval must be sought.

6. Implementation

6.1 Plan for implementation

The Information Governance Manager will ensure that this policy is available to all directorate managers within the Trust. It is then their responsibility to ensure that all staff groups within their area are directed to this policy. Mandatory Information Governance training covers the secure transferral of information and this is promoted within the trust on a regular basis.

6.2 Dissemination

This policy will be available on the Trust Intranet and a publication in the Daily Brief to inform staff of the update to the policy.

6.3 Training and awareness

The data security awareness online training is provided by NHS digital via ESR and all staff must completed this training on an annual basis. There is a paper version which reflects the online version provided for ancillary staff.

7. Monitoring and compliance

Departmental visits will be carried out by the Information Governance Team throughout the Trust to map data that is transferred.

Data transfers will be uploaded into the Information Governance Toolkit data mapping section and a report will be generated, showing the level of risk each transfer holds. Any actions/risks that arise from the departmental visits will be fed into the Information Governance Steering Group (IGSG) and monitored by the Information Governance Manager. High level risks will be added to the risk register if the IGSG deem it appropriate. Any reports of data transferrals which breach this policy will be dealt with by the Information Security Manager and Information Governance Manager. These events will be reported to the IGSG and actions monitored.

Page/ Section of Key Document	Key control:	Checks to be carried out to confirm compliance with the Policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting:
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Page 4	Departments where data is transferred on a regular basis will be data mapped to assess the risks associated with the transfer	Information collection for date mapping and results uploaded into the national Information Governance Training Tool	When updates or processes change within department	Information Governance Manager	Information Governance Steering Group	Updated Yearly or when processes change
Page 4	Incident reports to the IGSG	Investigations into data transfer breaches	Bi-Monthly reports to IGSG	Information Governance Manager	Information Governance Steering Group	Bi-Monthly (at least 5 times a year)

8. Policy Review

The Information Governance Manager will ensure that the policy will be updated with any new national guidance. This policy will be reviewed every two years by the Information Governance Steering Group.

9. References

References:	Code:
Information Security Policy	
Internet/Email Policy	
Data Protection Act 1998	
Acute Code of Conduct for Employees in Respect of Confidentiality	
NHS Code of Practice: Confidentiality	
NHS Code of Practice: Records Management	
Acute Corporate Records Management Policy	
Guidance for Sharing Personal Data (Posters available on Acute Intranet)	

10. Background

10.1 Equality requirements

No impact from the equality assessment

10.2 Financial Risk Assessment

No impact from the financial risk assessment

10.3 Consultation

The policy has been created in the Information Governance Manager with input from the IGSG members

10.4 Approval Process

This policy will be approved at the Information Governance Steering group. Minor changes can be approved by the SIRO via IGSG prior to the 2 year review

10.5 Version Control

See table below

Date	Amendment	By:
May 2009	Updated format into Trust Policy Template and added information to match new headings. National amendments have been incorporated.	Information Governance Manager
Nov 2012	Updated to include the 'New' safe haven guidance	Information Governance Manager
Dec 2014	Updated into New Trust Policy Template	Information Governance Manager
Jan 2016	Updated specified years (2014/2016) to cover current policy approval Updated reporting structure and approval process Updated reference section with updated trust policies Updated PCD appendix and reference to PID throughout policy	Information Governance Manager

	Included reference to the Pseudonymisation Policy	
May 2019	Minor update including, relevant dates and approval Appendices removed and available on the Information Governance Webpages	Information Governance Manager

Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		Yes/No	Comments
1.	**Does the Policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N/A	
4.	**Is the impact of the Policy/guidance likely to be negative?**	N/A	
5.	**If so can the impact be avoided?**	N/A	
6.	**What alternatives are there to achieving the Policy/guidance without the impact?**	N/A	
7.	**Can we reduce the impact by taking different action?**	N/A	

If you have identified a potential discriminatory impact of this key document, please refer it to Assistant Manager of Human Resources, 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 Assistant Manager of Human Resources.

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	None

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval