



Document Type: Policy		Unique Identifier: CORP/POL/061	
Document Title: Information Sharing		Version Number: 2.2	
Scope: Trust Wide		Status: Ratified	
Author / Title: Fiona Prestwood, Information Governance Manager		Classification: Organisational	
Replaces: Version 2.1, Information Sharing, Corp/Pol/061		Responsibility: Innovation, Information and Informatics (I3) Service	
Validated By: Information Governance and Data Quality Group		Head of Department: Andy Wicks, Chief Information Officer	
Ratified By: Procedural Document and Information Leaflet Group		Date: 04/07/2016	
Review dates may alter if any significant changes are made		Date: 20/07/2016	
Review Date: 01/07/2019			
Which Principles of the NHS Constitution Apply? Please list from principles 1-7 which apply 3 Principles		Which Staff Pledges of the NHS Constitution Apply? Please list from staff pledges 1-7 which apply 3 Staff Pledges	
Does this document meet the requirements of the Equality Act 2010 in relation to Race, Religion and Belief, Age, Disability, Gender, Sexual Orientation, Gender Identity, Pregnancy & Maternity, Marriage and Civil Partnership, Carers, Human Rights and Social Economic Deprivation discrimination? Yes			
Document for Public Display: Yes			
Reference Check Completed by.....Joanne Shawcross.....Date.....16/8/16.....			
To be completed by Library and Knowledge Services Staff			

CONTENTS

		Page
	BEHAVIOURAL STANDARDS FRAMEWORK	3
1	SUMMARY	4
2	PURPOSE	4
3	SCOPE	4
4	POLICY	4
4.1	Definitions	4
4.2	Risk to the Trust	5
4.3	Roles, Responsibilities and Accountabilities	5
4.4	Legal and Guiding Principles	6
4.5	Trust Approach to Sharing Information and Data	7
4.6	Information Sharing Gateway (ISG)	7
4.7	Sharing or Disclosing Information	8
4.7.1	Partner Organisations and Third Parties	8
4.7.2	Police	8
4.7.3	Solicitors	10
4.8	Restricting the Sharing of Personal Information	10
4.9	Contacts	10
5	ATTACHMENTS	11
6	OTHER RELEVANT / ASSOCIATED DOCUMENTS	11
7	SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS	11
8	DEFINITIONS / GLOSSARY OF TERMS	11
9	CONSULTATION WITH STAFF AND PATIENTS	11
10	DISTRIBUTION PLAN	12
11	TRAINING	12
12	AMENDMENT HISTORY	12
Appendix 1	Procedure For Patients Who Elect To Restrict The Sharing Of Their Personal Information	13
Appendix 2	Equality And Diversity Impact Assessment Tool	15

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

BEHAVIOURAL STANDARDS FRAMEWORK

To help create a great place to work and a great place to be cared for, it is essential that our Trust policies, procedures and processes support our values and behaviours. This document, when used effectively, can help promote a workplace culture that values the contribution of everyone, shows support for staff as well as patients, recognises and celebrates the diversity of our staff, shows respect for everyone and ensures all our actions contribute to safe care and a safe working environment - all of which are principles of our Behavioural Standards Framework.

Behavioural Standards Framework – Expectations ‘at a glance’

Introduce yourself with #hello my name is. . . 	Value the contribution of everyone	Share learning with others
Be friendly and welcoming	Team working across all areas	Recognise diversity and celebrate this
Respect shown to everyone	Seek out and act on feedback	Ensure all our actions contribute to safe care and a safe working environment
Put patients at the centre of all we do	Be open and honest	For those who supervise / manage teams: ensure consistency and fairness in your approach
Show support to both staff and patients	Communicate effectively: listen to others and seek clarity when needed	Be proud of the role you do and how this contributes to patient care

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

1. SUMMARY

Information sharing across organisational boundaries is essential to support patient care and to facilitate operational processes. Where direct patient care is concerned, it is often necessary for personal identifiable information, such as patient care information, to be shared but otherwise it is always preferable where possible to share information in an anonymised or pseudonymised format.

Data Protection Legislation and other standards such as the Caldicott Review set out specific rules and safeguards around the sharing of personal identifiable information. In order to ensure the information being shared is authorised, secure and meets legislative requirements, an Information Sharing Framework is used.

2. PURPOSE

The purpose of this policy is to define clear principles (and associated authorisation governance processes) about

- What Information / Data may and may not be shared, with whom, and for what purposes.
- Provide guidance on explicit requirements around data handling that ensures data is handled in a secure and confidential manner.
- Provide staff who use patient information with guidance about how to safeguard the confidentiality of the patient's information when the data is used for purposes other than direct patient healthcare.
- This policy is in line with the NHS Policy and the Information Commissioner's statutory Code of Practice.

3. SCOPE

This policy is principally concerned with the security of patient information when used for purposes other than direct patient care, but the principles and approaches apply to all personal information held by the Trust.

The policy applies to all full-time and part-time employees of the Trust, non-executive directors, contracted third parties (including agency staff and volunteers), students, trainees, individuals on secondment and other staff on placement with the Trust plus staff of partner organisations with approved access (such as Social Services).

4. POLICY

4.1. Definitions

Personal Data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This includes name, identification number, location data or online identifier.

Sensitive Personal Data / Special Categories of Personal Data is more sensitive personal data that requires more protection and includes;

- race;
- ethnic origin;

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Anonymised Information is where all elements of potential identifiers are removed completely so that it does not identify an individual.

Pseudonymised Information is where data is anonymised but retains a single key such as a code or reference number, known only to the provider of the information so that when it is shared, the provider can link back to the individual.

4.2 Risk to the Trust

Data and information collected, analysed, stored, communicated and reported may be subject to theft, misuse, loss and corruption.

Poor education and training, misuse, and breach of security controls of information systems may result in data and information being put at risk, may be used to misrepresent the Trust and result in the ineffective use of Trust’s resources. Information Security incidents can give rise to embarrassment, liability to third parties, noncompliance with Standards and legislation as well as possible judgements and financial penalties against the Trust.

4.3 Roles, Responsibilities and Accountabilities

Senior Information Risk Officer (SIRO) is responsible for ensuring that there are up-to- date and adequate Information Sharing Agreements in place for the sharing of Information across organisational boundaries.

Caldicott Guardian is responsible for overseeing all arrangements, protocols and procedures where confidential patient information may be shared.

Data Protection Officer is responsible for ensuring the organisations compliance with the data protection legislation

Information Asset Owners are responsible for ensuring that any Information Sharing Protocols that relate to their assets are maintained and any issues or risks are reported to the SIRO.

Information Governance will provide support and expertise to the organisation in the development and implementation of Information Sharing across organisational boundaries.

Managers are responsible for making staff with access to information aware of Information Governance issues, policies and procedures. This will be done through induction processes (corporate and local), the provision of training and day-to-day management of individuals.

All staff are responsible for the information that they pass on. If there is any doubt about whether

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

it is appropriate to share information, staff must always check with their line manager. The Trust requires all employees to comply with the Procedures and Guidelines which are in place to implement this policy.

4.4 Legal and Guiding Principles

The sharing of personal identifiable information is subject to three major legal considerations

Common Law Duty of Confidentiality¹ which is built on case law. Information that is confidential in nature should not be used or disclosed further, except as originally understood or with the data subject’s permission. Information contained in medical records is generally considered to be confidential. Therefore information should only be shared with consent or where information can be pseudon/anonymised.

Human Rights Act 1998² This Act incorporates the European Convention of Human Rights into our domestic law. Article 8 of the Convention states that “Everyone has the right to respect for his private and family life, his home and his correspondence”. This right is not absolute, however any interference with an individual’s privacy must be justified. Therefore sharing must be shown to be undertaken in accordance with the law, in the pursuit of a legitimate aim and necessary in a democratic society

General Data Protection Legislation³ and **Data Protection Act 2018**⁴ provides the framework governing the processing of personal data. This includes holding, obtaining, recording, using and disclosing information and applies to all media from paper to images. The principles are:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.”

These are supplemented in the NHS with guiding principles based on the

Caldicott Principles⁵

1. Justify the purpose(s) for using personal confidential data
2. Don’t use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

NHS Confidentiality Code of Practice¹

The NHS is committed to the delivery of a first class confidential service. This means ensuring that all patient information is processed fairly, lawfully and as transparently as possible so that the public:

- understand the reasons for processing personal information;
- give their consent for the disclosure and use of their personal information;
- gain trust in the way the NHS handles information and;
- understand their rights to access information held about them.

4.5 Trust Approach to Sharing Information and Data

When considering information sharing, we must;

- Ensure that there are agreed processes for authorising the use of personal confidential data. Where there is no approved process, the Caldicott Guardian holds responsibility for authorising (or not) the release of personal identifiable information / data
- Meet the Trust’s legal duties and requirements
- Ensure personal data will only be used for authorised primary use (direct patient care related) purposes. Secondary uses must follow national pseudonymisation rules
- Ensure data will be transferred via an approved secure process (technical and organisational measures) to prevent loss or unauthorised access. Electronic transfers will be encrypted
- Where possible / appropriate have individual consent to sharing information (for example within approved Research Projects)
- Access to personal confidential data will be
 - On a “need to know” basis
 - The minimum amount of information required available
 - With secure system (technical and organisational measure) in place
- Ensure sharing outside the Trust is recorded and risk assessed using the Information Sharing Gateway System (ISG) (see Section 4.6.)
- Ensure publication rules will be adopted to ensure confidentiality issues, data sources, data quality; audit trails are sufficiently addressed/ documented in published information

Ensure aggregate data will usually be available to the public unless falling under Freedom of Information Act exemptions⁶

4.6 Information Sharing Gateway (ISG)

The Information Sharing Gateway (ISG) has been developed by a sub-group of organisations in the Lancashire & Cumbria area to improve and modernise the administration and risk assessment of information sharing in the public sector. It has been designed by IG specialists, for IG specialists, to support their IG reporting on data flows and information sharing (principally for Information Governance Toolkit). It is developed with the needs of interoperable systems in mind, a ‘next generation’ information sharing framework that will adequately support electronic information sharing across care boundaries in a way that current, paper-based systems cannot.

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

The purpose of this system is to provide assurance that the information being shared, managed and processed will be done so in such a way that is Data Protection Legislation compliant. While centralising and sharing key resources in a way that is accessible and transparent. All current and new information sharing will be recorded on the Information Sharing Gateway.

4.7.1 Partner Organisations and Third Parties

Any sharing with partner organisation e.g. another acute Trust or third party e.g. private hospital must be go through an Information Governance Assurance process to ensure that the information being shared, managed and processed will be Data Protection Legislation compliant.

The assurance process will include

- Mapping the flow of the data from one organisation to another
- Assessment of the processes, procedures, training and security arrangements of the receiving organisation
- Assessment of privacy documented in a Data Protection Impact Assessment (DPIA)⁷
- Assess and define each organisations role and responsibilities when working with the data and whether a data processing agreement is needed

All this will be recorded on the Information Sharing Gateway and electronically agreed / signed by each partner organisation. Parties should contact the Information Governance Team (details in 4.8 Contacts) to progress an Information Sharing.

4.7.2 Police

The police do not have a general or automatic right to access personal identifiable information or access health records. In the absence of a legal requirement personal identifiable information must not disclosed to the police unless either there is explicit consent from the patient or it is clearly in the public interest to override the patient’s duty of confidentiality.

The legal requirements would be

- **Court Order** – this will state that the Trust must disclose the health record (or a part of it) to the police and the record must be disclosed in accordance with the terms of the order. If the Court Order requires immediate disclosure, review the order carefully identifying the relevant party, information to be disclosed and the date the disclosure needs to take place, as well as contacting the Legal Department or Duty Manager. Court orders with future dates should be passed appropriate area (Legal Department, Medical Records and the Safeguarding Team) for processing.
- **Road Traffic Act 1998⁸** – Section 172 of the Act requires the Trust to respond to a request from the police for any information that may lead to the identification of the driver of a vehicle where the driver of a vehicle is alleged to have committed an offence under the Act. Only information which allows someone to be identified should be released under this provision. No other information from the health records should be disclosed.
- **Police and Criminal Evidence Act 1984 (PACE)⁹** where the police are lawfully on the Trust’s premises for example with the Trust’s consent or in accordance with a valid search warrant under Section 19 of the Act the police may seize health records where
 - The records may be evidence in relation to a crime
 - The police have reasonable grounds for believing that it is necessary to seize health records in order to prevent evidence from being concealed, lost, altered or destroyed
 It is for the police to decide whether the requirements of section 19 are satisfied, if they

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

inform the Trust they are relying on section 19 PACE to seize health records, records may be disclosed. Where original Health records are to be seized to prevent evidence tampering a copy should be made before the records are disclosed and the Trust's legal department informed immediately. For other purposes the police should be provided with a copy of the notes, so the records can be used to treat patients.

- **Search Warrants** – on rare occasions the police may obtain a search warrant which permits them to enter Trust premises, conduct a search and seize records. The police do not necessarily have to give advance warning. In all cases you must contact the Trust's legal department or duty manager immediately and should not obstruct the search
- **Patient Consent** - this is where a patient has consent to their information being shared with the police, this must be clearly documented and ideally a consent form signed by the patient concerned. In all scenarios involving consent, you should satisfy yourself that
 - patient has capacity to give consent
 - patient consent is not being exceeded
- **Disclosure in the Public Interest** – request made under Section 29 of the Data Protection Legislation, the Trust must be satisfied that
 - Disclosure is for purposes of an investigation or enquiry being conducted by the police for a serious offence for example murder, manslaughter, rape, serious assault, abduction, child abuse or other cases where an individual has suffered harm
 - Seeking the patient's consent would be likely to prejudice the police investigation or enquiry, it is not possible or practicable or that it would defeat the purpose of the disclosure e.g. seeking a patient's address so they can apprehend them
 - Only the minimum amount of information required is being disclosed

So the Trust can make an informed decision the police must confirm

- What information is required
- Why the information is required, what crime is under investigation and what the information will be used for
- Whether the patient has consented? If not, why not?
- Why does the Trust need to disclose the information, could the information be obtained from another source and how would the enquiry or investigation be prejudiced if not disclosed

The police must provide a 'form (it is sometimes known as a DP1 form this will depend on the constabulary) which will record the request, note responses and should be signed by a senior police person.

The written request should be retained with details of what has been disclosed and for what purpose with a police signature confirming information will be kept confidential and only used for the purpose agreed.

You are not legally required to disclose information in the public interest, seek advice or ask the police to apply for a court order.

Always seek clarification if at any point of the process aspects become uncertain, contact the Trust's Legal Department or Duty Manager to seek clarification

4.7.3 Solicitors

Information can only be disclosed to solicitors where the patient has consented to the information being shared or in response to a court order. Only the information requested must be disclosed.

4.8 Restricting the Sharing of Personal Information

There will be circumstances where

- an individual requests that their personal information is not shared with another organisation,

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

for a purpose other than direct healthcare, for example audit, research and secondary use. Follow the process in Appendix 1 to update Lorenzo, arrange for a note to be placed on the patient's paper case notes and apply the necessary codes to the patient's CDS record to reflect their request

- an individual requests that no personal information is shared at all. Whilst we would always respect their request, they must be made aware of the consequences as this could affect the safe provisions of their care. For example, we would be unable to contact their GP to provide an immediate discharge summary or refer them to specialist service without their explicit consent. A meeting should be arranged with the individual to discuss. Follow the process in Appendix 1 to update Lorenzo, the patient's paper case notes and apply the necessary codes to the patient's CDS record to reflect their request.

4.9 Contacts

Information Governance	Information.Governance@mbhci.nhs.uk
I3 Service Desk	servicedesk@mbhci.nhs.uk Extension: 46000 or 01524 516000
Legal Department	Claims.UHMB@mbht.nhs.uk Extension: 45083
Site Duty Manager	Via Switchboard

5. ATTACHMENTS	
Number	Title
1	Procedure For Patients Who Elect To Restrict The Sharing Of Their Personal Information
2	Equality & Diversity Impact Assessment Tool

6. OTHER RELEVANT / ASSOCIATED DOCUMENTS	
Unique Identifier	Title and web links from the document library

University Hospitals of Morecambe Bay NHS Foundation Trust	ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019
Title: Information Sharing	
<i>Do you have the up to date version? See the intranet for the latest version</i>	

7. SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS

References in full

Number	References
1	DoH The Common Law Duty of Confidentiality. Available at: http://webarchive.nationalarchives.gov.uk/+/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_5803173 (accessed 16.8.16) See also Department of Health and Social Care (2003) Confidentiality: NHS Code of Practice. Available at: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice (accessed 16.8.16)
2	Great Britain (1998) Human Rights Act 1998. Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents (accessed 16.8.16)
3	General Data Protection Regulation (GDPR) (2016) Regulation (EU) 2016/679. Available at: https://gdpr-info.eu/ (accessed 16.8.16)
4	Great Britain (2018) Data Protection Act 2018. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 16.8.16)
5	Department of Health. (1997) Report on the Review of Patient-Identifiable Information. Available at: http://webarchive.nationalarchives.gov.uk/20130124064947/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf (accessed 16.8.16)
6	Great Britain (2016) Freedom of Information Exemptions. Available at: http://www.nationalarchives.gov.uk/documents/information-management/freedom-of-information-exemptions.pdf (accessed 16.8.16)
7	Information Commissioner's Office (ico) Data Protection Impact Assessments. Available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ (accessed 16.8.16)
8	Great Britain (1988) Road Traffic Act 1988. Available at: https://www.legislation.gov.uk/ukpga/1988/52/contents (accessed 16.8.16)
9	Great Britain (1984) Police and Criminal Evidence Act 1984. Available at: https://www.legislation.gov.uk/ukpga/1984/60/contents (accessed 16.8.16)
Bibliography	
BS ISO/IEC 27002:2005 – BS 7799-1:2005 – Information Technology – Security techniques – Code of practice for information security management	
Great Britain (2000) Freedom of Information Act 2000. Available at: https://www.legislation.gov.uk/ukpga/2000/36/contents (accessed 16.8.16)	
Great Britain (1990) Access to Health Records Act 1990. Available at: https://www.legislation.gov.uk/ukpga/1990/23/contents (accessed 16.8.16)	
Great Britain (2000) Freedom of Information Act 2000. Available at: https://www.legislation.gov.uk/ukpga/2000/36/contents (accessed 16.8.16)	
Department of Health and Social Care (2016) Records management code of practice for health and social care. Available at: https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care (accessed 16.8.16)	

University Hospitals of Morecambe Bay NHS Foundation Trust	ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019
Title: Information Sharing	
<i>Do you have the up to date version? See the intranet for the latest version</i>	

8. DEFINITIONS / GLOSSARY OF TERMS	
Abbreviation or Term	Definition

9. CONSULTATION WITH STAFF AND PATIENTS		
Enter the names and job titles of staff and stakeholders that have contributed to the document		
Name	Job Title	Date Consulted
Dan Willis	LSMS	

10. DISTRIBUTION PLAN	
Dissemination lead:	Fiona Prestwood
Previous document already being used?	Yes
If yes, in what format and where?	Word document on Procedural Document library
Proposed action to retrieve out-of-date copies of the document:	Copy removed and replaced with this document
To be disseminated to:	
Document Library	
Proposed actions to communicate the document contents to staff:	Include in the UHMB Weekly News – New documents uploaded to the Document Library

11. TRAINING		
Is training required to be given due to the introduction of this policy? No		
Action by	Action required	Implementation Date

University Hospitals of Morecambe Bay NHS Foundation Trust	ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019
Title: Information Sharing	
<i>Do you have the up to date version? See the intranet for the latest version</i>	

12. AMENDMENT HISTORY				
Version No.	Date of Issue	Page/Selection Changed	Description of Change	Review Date
1.0	09 May 2012	None	Final version after consultation with UHMB IAOs, IGSG, Risk and Safeguarding Leads	May 2014
1.1	May 2014		Review and update of policy	May 2016
2.0	July 2016	All reviewed and sections added	Review and update by IG Team to include section of sharing and disclosing of information Reviewed by IG Group , I3 RMF, Legal Team and Hills Dickinson Solicitors	July 2019
2.1	06/10/2017	Page 3	BSF page added	01/07/2019
2.2	May 2018	Section 4.1 Definitions Section 4.4 Legal and Guiding Principles	Update to reflect changes in Data Protection Legislation	01/07/2019

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

Appendix 1: Procedure for Patients Who Elect To Restrict the Sharing Of Their Personal Information

The following sets out the procedure to be adopted where a patient makes a request to restrict the sharing of their patient information, the information will fall into the following groups

- Direct provision of healthcare within UHMB
- Purposes other than provision of direct healthcare within UHMB e.g. Audit, research
- Direct provision of healthcare outside UHMB
- For secondary user or purpose other than healthcare e.g. SUS, CDS

We need to seek explicit consent from the patient to use their identifiable data for purposes other than those directly associated with their care and treatment.

Take the following actions:

Lorenzo Record: *add an alert category 'behavioural'*

Contact Health Informatics Service Desk and log a call with Application Support Team.

'This patient has declined to have their personal information held by UHMB shared for purposes other than direct healthcare. Please seek explicit consent from the patient to share identifiable information internally for non-healthcare purposes, or with any external agency, unless there is a specific exemption under Data Protection Legislation. For further guidance please contact Information Governance on information.governance@mbhci.nhs.uk or call 01524 46438/46166'

Paper Case-notes

Contact Medical Records Service Manager to have a note attached to the front of the casenote

'This patient has declined to have their personal information held by UHMB shared for purposes other than direct healthcare. Please seek explicit consent from the patient to share identifiable information internally for non-healthcare purposes, or with any external agency, unless there is a specific exemption under Data Protection Legislation. For further guidance please contact Information Governance on information.governance@mbhci.nhs.uk or call 01524 46438/ 46166'

Commissioning Data Set

Contact the Corporate Information Unit Manager or System Development Manager for them to mark the patients CDS record with the following detail

Identity withheld: 03 Record anonymised at the request of the patient.

This strips out NHS no, postcode and DOB from information provided as part of the Commissioning Data Set

Patient declines to have their personal information shared with anyone

Occasionally patients may decline to have their information shared at all; whilst we would always respect their wishes, they must be made aware that this could affect the safe provision of their care and treatment. For instance, we would be unable to do the following without their explicit consent: Contact their GP to provide an Immediate Discharge Summary or refer them on for specialist treatment (tertiary referral) or send away a Pathology test to a specialist centre.

In these circumstances a meeting should be arranged with the patient to discuss the

University Hospitals of Morecambe Bay NHS Foundation Trust	ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019
Title: Information Sharing	
Do you have the up to date version? See the intranet for the latest version	

implications of doing of not sharing with anyone. The patient should sign an agreement which will be uploaded to Lorenzo, Paper Case-notes and the necessary codes applied to the patient's CDS record.

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		

Appendix 2: EQUALITY & DIVERSITY IMPACT ASSESSMENT TOOL

		Yes/No	Comments
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	• Age	No	
	• Disability	No	
	• Race	No	
	• Sex	No	
	• Religious belief – including no belief	No	
	• Sexual Orientation	No	
	• Gender reassignment	No	
	• Marriage and civil partnership	No	
	• Pregnancy and maternity	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination are there any exceptions - valid, legal and/or justifiable?	No	
4.	Is the impact of the policy/guidance likely to be negative?	No	
4a	If so can the impact be avoided?		
4b	What alternative are there to achieving the policy/guidance without the impact?		
4c	Can we reduce the impact by taking different action?		

For advice in respect of answering the above questions, and / or if you have identified a potential discriminatory impact of this procedural document, please contact the relevant person (see below), together with any suggestions as to the action required to avoid/reduce this impact.

For Service related procedural documents: Lynne Wyre, Deputy Chief Nurse & Lead for Service Inclusion and Diversity

For Workforce related procedural documents: Karmini McCann, Workforce Business Partner & Lead for Workforce Inclusion and Diversity.

University Hospitals of Morecambe Bay NHS Foundation Trust		ID No. Corp/Pol/061
Version No: 2.2	Next Review Date: 01/07/2019	Title: Information Sharing
<i>Do you have the up to date version? See the intranet for the latest version</i>		