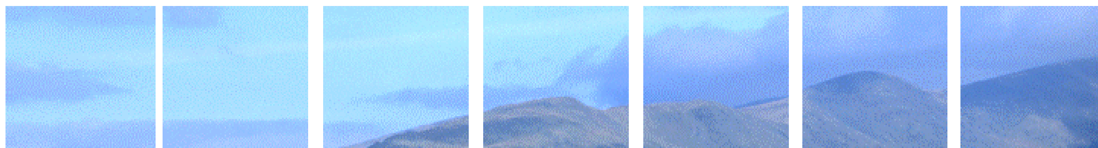
University Hospitals of Morecambe Bay **NHS**
NHS Foundation Trust



Document Type: **Policy**	**Unique Identifier:** CORP/POL/056
Document Title: **Privacy Monitoring**	**Version Number:** 1.4 **Status:** Ratified
Scope: Trust Wide	**Classification:** Organisational
Author / Title: Sue Wightman - Privacy Officer	**Responsibility:** Innovation, Information and Informatics (I^3) Service
Replaces: Version 1.3, Privacy Monitoring, Corp/Pol/056	**Head of Department:** Andy Wicks, Chief Information Officer
Validated By: Information Governance Group	**Date:** 09/11/2015
Ratified By: Procedural Documents and Information Leaflet Group	**Date:** 18/11/2015
Review dates may alter if any significant changes are made	**Review Date:** 01/06/2019 (Review date extended 054/2019)
Which Principles of the NHS Constitution Apply? **Please list from principles 1-7 which apply** 3	**Which Staff Pledges of the NHS Constitution Apply?** **Please list from staff pledges 1-7 which apply** 3
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…………Frances Sim………………..Date……24.11.15……. **To be completed by Library and Knowledge Services Staff**	

Contents

BEHAVIOURAL STANDARDS FRAMEWORK ... 3
1. SUMMARY ... 4
2. PURPOSE ... 4
3. SCOPE ... 4
4. POLICY ... 4
4.1 Roles and Responsibilities ... 5
4.1.1 Privacy Officer ... 5
4.1.2 Workforce and Organisation Development ... 5
4.1.3 IG Team - Information Governance Team ... 5
4.2 Monitoring Preliminary Enquiries and Privacy Investigations ... 5
4.2.1 Monitoring ... 5
4.2.2 Preliminary Enquiries ... 6
4.2.3 Privacy Investigation ... 6
4.2.4 Post Investigation ... 6
4.3 Reporting ... 7
4.3.1 Partner Organisations ... 7
4.3.2 Subject Access Request / Complaint Reports ... 7
4.3.3 Information Governance Groups ... 7
4.4 Awareness and Training ... 7
4.5 Contacts ... **Error! Bookmark not defined.**
5. ATTACHMENTS ... 8
6. OTHER RELEVANT / ASSOCIATED DOCUMENTS ... 8
7. SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS ... 8
8. DEFINITIONS / GLOSSARY OF TERMS ... 8
9. CONSULTATION WITH STAFF AND PATIENTS ... 9
10. DISTRIBUTION PLAN ... 9
11. TRAINING ... 9
12. AMENDMENT HISTORY ... 9
Appendix 1: EQUALITY & DIVERSITY IMPACT ASSESSMENT TOOL ... 10

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'

1. SUMMARY

The Trust is committed to safeguarding the privacy of patient information and in order to do this, has implemented measures to comply with our legal obligations. Privacy Watch is a new monitoring system which will detect potential instances of unauthorised access to patient information held within electronic information systems. It will track these systems in real time and highlight possible breaches. This in turn will

- Simplify the analysis of audit files
- Make it easier to generate reports
- Detect potentially unauthorised access to electronic systems which hold patient information
- Highlight unusual or suspicious activity for further investigation.
- Enable investigation of accesses made by specific members of staff

Our patients have the right to expect that the information we hold about them will be kept confidential and all staff are contracted to following the Trust's Acceptable Use Policy, Confidentiality Policy and the Policy for Information Security.

2. PURPOSE

This policy is intended for use by University Hospitals of Morecambe Bay Information Governance (I3) staff and sets the policy for effectively co-ordinating and managing the viewing of Electronic Patient Record (EPR), GP Detailed Care Record (DCR) and Summary Care Record (SCR). This Policy is to ensure that the processes are understood and followed from the initial decisions of who should view, the responsibilities of individual staff members through to the duties of the Privacy Officer within the Trust and the expectation of spot check auditing to ensure the viewing of patient records within the Trust is transparent and the resource is being used in an effective way.

It is essential, for the benefit of all concerned, that this policy is applied consistently in all cases, regardless of the position or designation of the staff member involved. Compliance with the Data Protection Act[1] is a legal requirement and the Trust, in common with all NHS organisations, must be able to demonstrate that non-compliance is dealt with appropriately.

3. SCOPE

This document is for the use of staff in the Innovation, Information and Informatics (I^3) Service of University Hospitals of Morecambe Bay Trust (UHMB) and any relevant associated clinical staff.

Currently Privacy Watch is for Trust Staff with access to the GP Summary Record, the SCR and the Trusts EPR system

All staff employed by UHMB and authorised external users will be monitored.

4. POLICY

'Privacy Watch' is designed to help provide assurance to partner organisations (e.g. GP Practices) and the public (patients) that

- the Trust's access to their electronically held information, is being utilised to aid the delivery of direct health care, and that organisation staff are not accessing records without a legitimate reason
- Complaints from patients or staff who believe that a member of staff has inappropriately accessed their record are investigated in line with the 12th commitment of the Care Record Guarantee[2]: *"If you believe your information is being viewed inappropriately we will investigate and report our findings to you. If we find that someone has deliberately accessed records about you without permission or good reason, we will tell you and take action. This can include disciplinary action, which could include ending a contract, firing an employee or bringing criminal charges."*

4.1 Roles and Responsibilities

4.1.1 Privacy Officer

Will monitor and audit access to the use of Trust Systems and investigate alerts, complaints or incidents where access to Trust Systems may not have been legitimate.

Provide assurance to relevant data controllers that the use of systems complies with the standards and legislation relating to the use, collection and disclosure of personal information.

Prepare regular privacy reports to include privacy violation. Engage with staff throughout Morecambe Bay to promote awareness and develop departmental relationships.

4.1.2 Workforce and Organisation Development

Will ensure that Privacy Investigations are properly handled, supporting Line Managers or lead through the Trust's disciplinary process.

Will support the Privacy Officer with advice concerning requirements for Disciplinary Panel and the Trust's disciplinary process

4.1.3 IG Team - Information Governance Team

Support the Privacy Officer where required

Advise the Privacy Officer on Information Governance and Data Protection issues and relevant policies and procedures

1.

4.2 Monitoring Preliminary Enquiries and Privacy Investigations

The Privacy Officer will follow their defined and agreed procedures; these are available upon request and form part of the Privacy Monitoring Standard Operating Procedure.

2. Please note this document is currently an evolving document and is regularly reviewed and updated.

4.2.1 Monitoring

3. The Trust's Privacy Officer will be responsible for monitoring and auditing the reports generated by Privacy Watch, monitoring requests or Subject Access Requests or complaints made.

The monitoring will be aiming to highlight exceptions which for the purpose of this policy are defined as any access to a record which appears to fall outside of expected

behaviours e.g. record accessed but the patient has no open episode of care. Any exceptions which appear to be a potential privacy breach because access is unclear or questionable will require the Privacy Officer to perform preliminary enquiries

The system will monitor and have the ability to check;

- Records are access when there is no open episode of care
- Staff accessing their own record
- A patient concerns that their record has been accessed inappropriately
- Staff are accessing a friend or family member record
- High profile cases which may be of interest to staff e.g. VIPs, celebrates and Senior Trust staff

4.2.2 Preliminary Enquiries

The preliminary enquiry will determine whether there has been a legitimate business reason to access the record that has been flagged.

If the access is found to be still to be unclear, questionable or unjustifiable the Privacy officer may extend to a full privacy investigation should the confidentiality of the record be believed to have been breached.

All responses should be made in writing (email / letter via internal mail) and stored electronically.

All outcomes will be documented.

4.2.3 Privacy Investigation

All privacy investigations that result in a confirmed privacy breach will be logged on the Trust's Incident Management System (Safeguard) and the member of staff's Line Manager or Lead and the department's HR Business Partner will be informed of the privacy breach.

All responses should be in writing (email / letter via internal mail) these will be form part of investigation findings.

Where it can be evidenced that a staff member has repeatedly accessed the health records and personal information of others, there is an expectation that this would be dealt with through the Trust's formal disciplinary process and depending on the circumstances, may result in formal disciplinary action including dismissal.

The findings of the investigation will be collated and a report produced which will be reviewed by a member of the Information Governance (IG) Team and disseminated to the member of staff's line manager / lead and HR Business Partner. The report and evidence will be uploaded to Safeguard.

4.2.4 Post Investigation

The Privacy Officer will provide the Line Manager / Lead and HR Business Partner with support where required to interpret the report provided.

The Privacy Officer will ensure that the outcome of any formal Trust disciplinary procedure

is documented to enable reporting to partner organisations and other bodies to be complete and accurate.

4.3 Reporting

Reports will be generated and disseminated as necessary. These may include audit reports to provide assurance to GP Practices around the use of their Patient's SCR and DCR. Reports for members of the public who have made a request to see out who has accessed their record. Anonymised incident reports for the IG team outlining any Privacy investigations which have taken place and their outcomes.

4.3.1 Partner Organisations

The Privacy Officer will provide partner organisation with audit reports to provide assurance that access to the data they have provided is being used for agreed purpose. The report will include details of the accesses, number of identified exceptions and the outcome of any investigations. The frequency and the format of the reports will dependant on the partner organisations requirements.

4.3.2 Subject Access Request / Complaint Reports

The Privacy Officer will provide a summary of their findings to the requestor after it has been reviewed by IG Team and relevant staff. As these reports may contain information on individual NHS Staff, in order to protect their rights and privacy (as per the Data Protection Act 2018[1]), the Trust may not release staff details depending on the request made, a reason for non-disclosure will be provided to the requestor

4.3.3 Information Governance Groups

The Privacy Officer will provide the IG Team with anonymised details of investigations undertaken, their outcomes and themes. This will be incorporated into the IG Group monthly Incident Summary Report

4.4 Awareness and Training

The Privacy Officer will provide communications, awareness and training relating to Privacy as part of the Privacy Monitoring. The content will be dependent on the audience

4.5 Contacts

Information Governance	Information.Governance@mbhci.nhs.uk
Privacy Watch	Privacy.Watch@mbhci.nhs.uk

5. ATTACHMENTS	
Number	**Title**
1	Equality and Diversity Impact Assessment Tool

6. OTHER RELEVANT / ASSOCIATED DOCUMENTS	
Unique Identifier	**Title and web links from the document library**
Corp/Pol/116	Acceptable Use Policy for Information Communication and Technology (ICT) Systems and Equipment http://uhmb/cs/tpdl/Documents/CORP-POL-116.docx
Corp/Pol/015	Data Protection and Confidentiality http://uhmb/cs/tpdl/Documents/CORP-POL-015.docx
Corp/Pol/069	Policy for Information Security http://uhmb/cs/tpdl/Documents/CORP-POL-069.docx
MRec/SOP/001	Managing Access to Health Records and Image Requests http://uhmb/cs/tpdl/Documents/MREC-SOP-001.docx
MRec/SOP/003	Safe and Secure Storage of Patient Records http://uhmb/cs/tpdl/Documents/MREC-SOP-003.docx

7. SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS References in full	
Number	References
1	Great Britain (2018). Data Protection Act 2018. Available from: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 10/07/2018)
2	The National Information Governance Board for Health and Social Care (2011). The Care Record Guarantee : Our Guarantee for NHS Care Records in England. version 5. [Online] Available at: http://tinyurl.com/o8n4x5p (accessed 24.11.15)

8. DEFINITIONS / GLOSSARY OF TERMS	
Abbreviation or Term	**Definition**
EPR	Electronic Patient Record
DCR	GP Detailed Care Record – read only view of the electronic GP record available via Lorenzo
SCR	Summary Care Record – read-only view of the electronic GP record available via Lorenzo and the NHS Spine

9. CONSULTATION WITH STAFF AND PATIENTS	
Name	**Job Title**
Fiona Prestwood	Information Governance Manager
Sue Wightman	Privacy Officer
Helen Speed	Information Systems Manager (IG Lead)
Carol Hogarth	Information Governance Officer
Gail Martin	Information Security Officer
I^3 Risk Management Forum	Members of the Group
Information Governance Group	Members of the Group

10. DISTRIBUTION PLAN	
Dissemination lead:	Sue Wightman
Previous document already being used?	No
If yes, in what format and where?	n/a
Proposed action to retrieve out-of-date copies of the document:	n/a
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? *Yes / No * Please delete as required

Action by	Action required	Implementation Date

12. AMENDMENT HISTORY				
Version No.	**Date of Issue**	**Page/Selection Changed**	**Description of Change**	**Review Date**
1.1	05/10/2017	Page 3	BSF page added	01/11/2018
1.2	10/07/2018	Page 7	Data Protection Act amended to 2018	01/11/2018
1.3	22/11/2018	Review Date	Review date extended. 161/2018	01/02/2019
1.4	19/03/2019	Front Cover	Review date extended form 054/2019	01/06/2019

Appendix 1: 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:**		
	• 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	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	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?**	n/a	
4b	**What alternative are there to achieving the policy/guidance without the impact?**	n/a	
4c	**Can we reduce the impact by taking different action?**	n/a	

If you have identified a potential discriminatory impact of this procedural document, please refer it to the HR Equality & Diversity Specialist, 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 HR Equality & Diversity Specialist, Extension 6242.