University Hospitals of Morecambe Bay NHS Foundation Trust

Document Type: **Policy**	**Unique Identifier:** CORP/POL/070
Document Title: **Information Risk**	**Version Number:** 2.3 **Status:** Ratified
Scope: Trust Wide	**Classification:** Organisational
Author / Title: Fiona Prestwood, Information Governance Manager	**Responsibility:** Innovation, Information and Informatics (I^3)
Replaces: Version 2.2, Information Risk**,** Corp/Pol/070	**Head of Department:** Andy Wicks, Chief Information Officer
Validated By: Information Governance Group	**Date:** 11/02/2016
Ratified By: Procedural Document and Information Leaflet Group	**Date:** 17/02/2016
Review dates may alter if any significant changes are made	**Review Date:** 01/05/2019 (Review date extended form 054/2019)

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……16.2.16…….

To be completed by Library and Knowledge Services Staff

CONTENTS		
		Page
	BEHAVIOURAL STANDARDS FRAMEWORK	3
1	SUMMARY	4
2	PURPOSE	4
3	SCOPE	5
4	POLICY	5
4.1	Legislation And Standards	5
4.2	Information Risk Appetite	5
4.3	Statement Of Management Intent	6
4.4	Roles And Responsibilities	6
4.4.1	Accounting Officer (CEO)	6
4.4.2	Senior Information Risk Officer (SIRO)	6
4.4.3	Information Asset Owners (IAO)	6
4.4.4	Information Asset Administrators	6
4.4.5	Governance Leads	6
4.4.6	Information Governance Team	7
4.4.7	All Staff	7
4.5	Information Sharing	7
4.6	Information Risk Management Assurance Framework	7
4.7	Information Risk Management Process	7
4.8	Risk Management Training	8
5	ATTACHMENTS	9
6	OTHER RELEVANT / ASSOCIATED DOCUMENTS	9
7	SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS	9
8	DEFINITIONS / GLOSSARY OF TERMS	10
9	CONSULTATION WITH STAFF AND PATIENTS	10
10	DISTRIBUTION PLAN	10
11	TRAINING	10
12	AMENDMENT HISTORY	11
Appendix 1	Process For Suspension Of Information System Access Privileges Where Training Is Out Of Date.	12
Appendix 2	Equality and Diversity Impact Assessment Tool	13

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 Information Security Management: NHS Code of Practice[1] states 'Effective Information Security Management is based upon the core principle of risk assessment and management'. This requires the identification and quantification of information security risks in terms of their perceived severity of impact and the likelihood of occurrence. Once identified, information security risks need to be managed on a formal basis.

2. PURPOSE

This policy sets out a framework for information risk management by establishing the accountability and responsibility arrangements for information risk identification, assessment and management. Information risk management is one component of the overall System of Internal Control and falls within the scope of the overarching UHMB Risk Management Strategy. Information risk management is critical to the implementation of an Information Security Management System. Information will not be managed separately from other business risks and will be considered as an element of the overall corporate governance framework.

The Information Risk policy will enable the Trust to:

- Provide protection to Trust information assets and reputation
- Establish and maintain a pro-active and systematic process of information risk management to support quality of decision making throughout the Trust
- Use information to support the organisation's commitment to promote the delivery of the highest possible standards of care
- Develop management plans and staff education and training about information risk, learning from incidents and issues that arise
- Meet legal and statutory requirements and demonstrate year on year improvement against the Information Governance Toolkit standards

From this point forward University Hospitals of Morecambe Bay NHS Foundation Trust will be known as UHMB or the Trust.

This policy sets out the approach by which UHMB will meet its responsibilities for the Information Risk Management of the Trusts Information Assets. The key characteristics of information Assets are that they:

- are identifiable and their ownership is assignable to an Information Asset Owner (IAO) within the organisation
- have 'value' to the organisation and contribute to satisfying its business objectives
- are not easily replaceable if lost or damaged beyond repair without significant new financial investment in time or resource
- form part of the organisation's overall asset inventory such that their business importance is understood and their risks are managed

Information Assets of value are those that are central to the efficient running of UHMB departments and include key information systems such as Lorenzo and Oracle Financials. Information Assets include:

- Personal Information content (patients and staff) in case notes, databases, audit data and reports
- System and process documentation (relating to computerised and non-computerised

systems) for example databases, training documentation, Standard Operating Procedures, Business Continuity Plans and Information Sharing Agreements
- Hardware and physical assets such as IT infrastructure, IT equipment and specialist areas and accommodation used for data processing
- Software such as application programs, systems, development tools and utilities which are used to process this data
- Services for example computing and communications, heating, lighting, power, air conditioning used for data processing
- People, their qualifications, skills, experience and expertise in the use of information systems

3. SCOPE

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 Legislation And Standards

The Trust will put policies and Procedures in place to ensure that it can fulfil all legal and regulatory obligations to maintain the security of their information assets.

These include, but are not limited to, responsibilities as defined in:
- The Data Protection Act (20188)[2]
- The UK Computer Misuse Act (1990)[3]
- The Caldicott Review of Patient Identifiable Information, (1997)[4]
- The Freedom of Information Act (2000)[5]
- The Information Security Management: NHS Code of Practice[1]
- Confidentiality – NHS Code of Conduct (2003)[6]
- Information Governance Toolkit

Staff are required to comply with this policy to conform with current legislation.

4.2 Information Risk Appetite

The Trust is not willing to accept information risks that may result in reputational damage, financial loss or exposure, major breakdown of information system or information integrity, significant incidents of regulatory non-compliance, potential injury to staff, patients, visitors or other people working on behalf of the Trust.

Where risk to information assets presents a potential clinical risk to patients, or where personal data is the information asset in question, the UHMB risk appetite is extremely low. Information risks should always be assessed for and state explicitly whether concomitant clinical risk is also present. Where information risk management plans are constrained by resource or time, priority should be given to treatment of information assets which present a significant clinical risk or comprise of or contain personal information.

4.3 Statement Of Management Intent

UHMB is committed to managing risk and creating a culture that promotes the delivery of the highest possible standards of care, by providing a proactive and systematic process of risk management to identify, analyse, minimise, control and, where possible eliminate any risks that may have an adverse impact on patients, staff or the organisation.

All staff have a responsibility to protect the security of confidential/sensitive information, particularly when it is person identifiable. All staff therefore should actively participate in identifying potential information risks in their areas and contribute to the implementation of appropriate action. This requires a structured approach with the clear identification of specific roles and responsibilities to ensure that risks can be managed across all levels in the organisation.

The UHMB risk management organisational structure is defined in the UHMB Risk Management Strategy. Specific aspects of this structure that relate to information risk are described in this policy.

4.4 Roles And Responsibilities

4.4.1 Accounting Officer (CEO) has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be managed as other corporate risks such as financial, operational, legal and reputational risks.

4.4.2 Senior Information Risk Officer (SIRO) is the executive director who is familiar with and takes ownership of the organisation's information risk policy, acts as advocate for information risk on the Trust Board. Ensuring that an overall culture exists that values and protects information within the organisation.

4.4.3 Information Asset Owners (IAO) are senior individuals involved in running the relevant business. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for acceptable use, annual risk assessment, business continuity, information security and information sharing.

4.4.4 Information Asset Administrators are responsible for the administration of specific Information Assets. Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up-to-date.

4.4.5 Governance Leads to understand and support the Organisation's plans to achieve a culture that values and protects information, to ensure staff understand the importance of effective information risk management and have access to and receive appropriate education and training. To ensure that the incident reporting mechanism is effective in supporting information risk management and lessons learnt.

4.4.6 Information Governance Team is responsible to the SIRO for the overall management of the information asset register and that each asset has an identified owner, administrator and IT lead. As well as supporting the organisation by providing technical

advice and expert support on risk management issues where appropriate

4.4.7 All staff are responsible for Information Security, the correct use of Information Assets and for the information that they share. Staff are required to follow Standard Operating Procedures where available and to use Information Systems and treat Information Assets in accordance with the training they have received and with Trust Policy. Staff have a responsibility to identify and address their own learning and development needs and for those of any staff that they manage. Failure to attend training appropriate to job role, including refresh and update training, may result in access to information systems being suspended or withdrawn (see Appendix 1).

4.5 Information Sharing

Information sharing is essential to support patient care and to facilitate operational processes, but must meet Data Protection Act[2] and Caldicott requirements and have due regard to the right to privacy of individual patients and staff.

UHMB are signatories to the Information Sharing Gateway Memorandum of Understanding which provides an overarching framework establishing common principles, standards and approaches for information sharing between signatory organisations.

Supporting documentation:
- *Information Sharing Policy*

4.6 Information Risk Management Assurance Framework

Information Risk Management will align with the Trust's Risk Management Strategy and therefore the responsibilities, definitions and processes contained within the Strategy apply to this Information Risk Policy.

Formal Information Risk Assurance will be provided to UHMB principally via, Information Governance Group, I3 Steering Group and I[3] Risk Management Forum which are all involved in oversight of the Information Governance Toolkit standards, but information risk is not exclusive to these groups.

Supporting documentation:
- *UHMB Risk Management Strategy*

4.7 Information Risk Management Process

The process of identifying information risks will be a proactive and systematic process of risk management to identify, analyse, minimise, control and, where possible eliminate any risks that may have an adverse impact on patients, staff or the organisation.

Information risks will be identified by

a. *Risk assessments* performed on all information assets owned and operated by the Trust by the assets Information Asset Owner (IAO). These occur;
- Annually to support the SIROs written advice on the statement of internal control to the Chief Executive
- At the implementation of new systems, applications or facilities that may impact on the assurance

- As a result of any significant changes, enhancements or upgrades to existing critical information systems or applications
- When the Trust's Integrated Risk Committee or Board of Directors requires assessment

b. *Reported Incidents* identifies an information risk which if not controlled or where possible eliminate may cause harm or have an adverse impact on patient, staff, the organisation or the asset itself

All information risks will be identified, quantified (general level of harm that could be reasonably caused if the information asset were to be compromised) and where appropriate mitigation action developed and implemented. Risk Mitigation must be commensurate with the level of risk – it does not need to remove the risk. It needs to be kept simple so it is manageable and can be communicated to staff.

The information risk will be recorded on the service's risk register held on the Trust's 'Safeguard' Incident and Risk Management System. All information risks will be managed together with all other identified risks for that service.

Information risks that are greater than or equal to 15 or where the risk is considered to be significant enough will be escalated as described in the UHMB Risk Management Strategy risk escalation process.

All information risks must be monitored and reviewed regularly to ensure that risk scores (pre and post mitigation) are accurate and up-to-date. Action plans need to be updated to reflect their current status. Where a risk score changes the information risk may require redefining or actions plans modified to reflect the change. Should a risk score increase significantly this should be escalated to the relevant forums for discussion.

At regular intervals the information risks recorded on the risk register should be audited to ensure that the scoring is consistent and that where risks are no longer of significance are tolerated or closed.

4.8 Risk Management Training

All staff who record information risks should undertake the recommended Information Governance training around Information Risk Management. Where these staff are IAOs they should undertake the Trust's IAO training.

5. ATTACHMENTS	
Number	**Title**
1	Process For Suspension Of Information System Access Privileges Where Training Is Out Of Date
2	Equality & Diversity Impact Assessment Tool

6. OTHER RELEVANT / ASSOCIATED DOCUMENTS	
Unique Identifier	**Title and web links from the document library**
Corp/Pol/069	Information Security Policy http://uhmb/cs/tpdl/Documents/CORP-POL-069.docx
Corp/Strat/001	Risk Management Strategy http://uhmb/cs/tpdl/Documents/CORP-STRAT-001.docx
Corp/Pol/061	Information Sharing Policy http://uhmb/cs/tpdl/Documents/CORP-POL-061.docx

7. SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS

References in full

No	References
1	DoH (2007) Information Security Management: NHS Code of Practice. [Online] Available at: http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf (accessed 16.2.16)
2	Great Britain (2018). Data Protection Act 2018. Available from: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed 10/07/2018)
3	Great Britain (1990) Computer Misuse Act 1990. [Online] Available at: http://www.legislation.gov.uk/ukpga/1990/18/contents (accessed 16.2.16)
4	DoH (1997) The Caldicott Committee. Report on the Review of Patient-Identifiable Information [Online] Available at: http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4068404.pdf (accessed 16.2.16)
5	Great Britain (2000) Freedom of Information Act 2000. [Online] Available at: http://www.legislation.gov.uk/ukpga/2000/36/contents (accessed 16.2.16)
6	DoH (2003) Confidentiality NHS Code of Practice. [Online] Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf (accessed 16.2.16)

Bibliography

ISO (2013) ISO/IEC 27002:2013 Information Technology – Security techniques – Code of practice for information security management. Available from: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533 (accessed 16.2.16)

ISO (2003) ISO/IEC 27001:2013 Information Technology – Security techniques – Information security management systems- Requirements. Available from: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534 (accessed 16.2.16)

8. DEFINITIONS / GLOSSARY OF TERMS	
Abbreviation or Term	**Definition**
UHMB	University Hospitals Of Morecambe Bay NHS Foundation Trust
CfH	Connecting For Heath
IAO	Information Asset Owner
DPA	Data Protection Act
ADR	Appraisal And Development Review
PDS	Personal Demographic Search
IG	Information Governance
SIRO	Senior Information Risk Owner

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**

10. DISTRIBUTION PLAN	
Dissemination lead:	Fiona Prestwood
Previous document already being used?	Yes
If yes, in what format and where?	
Proposed action to retrieve out-of-date copies of the document:	Updated on the Procedural Document Library
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 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**
Draft Version 0.1	February 2012		Draft document	
Draft version 0.2	February 29th 2012		Revised in light of consultation with IAOs, Governance leads and Interim Associate Director for Risk Management	
1.0	07 March 2012		Final	
2.0	11 February 2016		Document reviewed and supporting documents updated	
2.1	06/10/2017	Page 3	BSF page added	01/02/2019
2.2	10/07/2018	Throughout	Reference to Data Protection Act updated to 2018	01/02/2019
2.3	19/03/2019	Front Cover	Review date extended form 054/2019	01/05/2019

Appendix 1

Process For Suspension Of Information System Access Privileges Where Training Is Out Of Date.

There may be a risk of harm to patients if staff do not keep Information System training, such as Lorenzo training, up to date e.g. if this results in patients not receiving appointments for OPD or treatment, or incorrect recording of clinical information.
The Health Informatics Training Team will adopt the following process to invite staff to refresher training:

- Staff member is recalled to be retrained within time span agreed by the business
- Training Administration manages the list of staff due for retraining
- Email and letter is sent to the member of staff asking them to book onto training course
- Course is also added to the staff member to do list on TMS 'My Learning & Development'
- Staff member can self-book via TMS or ring Training Admin to book on course

Staff member should then:

- Book Training
- Attend training and pass Competency Assessment
- TMS is updated and training is valid until the next cycle of training is required for that area / functionality

If no booking is made:

- A weekly check is made on TMS and if no booking has been made, a reminder is sent out
- After an agreed length of time if still no booking made, a letter is sent to the line manager asking them to intervene
- If the member of staff still does not attend training, the line manager is notified by letter informing them that the roles will be removed from smart card until training is attended and competency established.
- Notification is sent to RA department to remove roles from card

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.