Reference Number: UHB 289 **Version Number:** 1	**Date of Next Review:** 22 Jun 2018 **Previous Trust/LHB Reference Number:** NA

Information Asset Management Procedure

Introduction and Aim

This document is written is support of the Information Governance Policy. It provides a mechanism to achieve and maintain appropriate protection of the Information Assets (IA) held by Cardiff and Vale University Health Board (the UHB). The aim is that all major IA are identified and are assigned owners with stated accountabilities and responsibilities and that there are clear lines of accountability within the management and governance framework.

The successful implementation of this procedure will address business and performance standards for example the requirement to meet Caldicott standards, Health and Care Standards (2015), and the Information Governance Toolkit Standards as far as possible in the Welsh context.

Objectives

The Information Asset Management procedure describes the mechanism the UHB will use to develop and maintain best practice in information asset management.

The UHB has seven key objectives in this area that are to:

- Provide a structure and organisation to deliver the information asset management agenda that effectively links the assurance responsibilities of the Senior Information Risk Officer (SIRO) and the Information Governance Sub Committee (IGSC) with the operational responsibilities of the Chief Operating Officer (COO).
- Implement and maintain a network of Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) with clear accountabilities and responsibilities documented within their job descriptions.
- Implement effective information governance processes.
- Develop and maintain standard operating procedures to support this overarching procedure.
- Train staff appropriately
- Provide adequate resources to maintain good practice

Provide exception reports to form the basis for improvements to the provision, support and development of Information Asset confidentiality, integrity and availability

Scope

This procedure applies to all of our staff in all locations including those with honorary contracts

Equality Impact	An Equality Impact Assessment has been completed for the

Assessment	overarching IG Policy. The assessment found that there was some impact on the equality groups mentioned in relation to communication. An action plan has been developed to address those areas.
Health Impact Assessment	A Health Impact Assessment has not been
Documents to read alongside this Procedure	Information Governance Policy Data Protection Act Policy Records Management Policy Data Quality Policy IT Security Policy Information Risk Management Procedure (to be completed) Risk Management Policy Guide to Incident Reporting Incident Management Investigation and Reporting. [Serious incidents] Access controls IM&T Security Breaches Business Continuity Management Security of Assets Off-site Mobile Computing Policy Remote Access Software Protocol
Approved by	Information Governance Sub Committee

Accountable Executive or Clinical Board Director	Medical Director
Author(s)	Head of Information Governance and Assurance

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.

Summary of reviews/amendments

Version Number	Date of Review Approved	Date Published	Summary of Amendments
1	22/06/2015	06/04/2016	New Procedure

Contents Page

1. Introduction

This document provides a mechanism to achieve and maintain appropriate protection of the organisation's Information Assets (IA). All major IA must be identified, have a responsible owner and maintenance responsibilities assigned. Accountability for assets helps to ensure that appropriate protection is maintained.

Information asset owners (IAOs) should be identified for all IA. Responsibilities for the maintenance of appropriate controls should be assigned to Information Asset Administrators (IAA). Responsibility for implementing and managing controls may be delegated by the IAOs, although accountability must remain with the nominated owner of the IA.

2. Purpose

The purpose of this procedure is to provide assurance to the Senior Information Risk Owner (SIRO) and ultimately the Board, that appropriate frameworks are in place to ensure robust Information Security, Information Risk, Information Business Continuity and Data Quality controls are in place to support the UHBs policies for clinical care, business and legal requirements and patient experience.

3. Information Assets

Information Assets are those that are central to the efficient running of departments within the UHB i.e. patient, finance, staff employment, stock control etc. Information Assets will also include the computer systems, network hardware and software which are used to process this data.

Non-computerised systems holding information must be asset registered with relevant file identifications and storage locations.

There are six main categories of information asset:

- Information – this includes databases, system documentation and procedures, archive media and data
- Software – this includes application programs, systems, development tools and utilities

- Physical – this includes infrastructure, equipment, furniture and accommodation used for data processing
- Services – including computing and communications, heating, lighting, power, air conditioning used for data processing
- People – including qualifications, skills and experience in the use of information systems
- Other – for example the reputation and image of the UHB

4. Role: Information Asset Owner (IAO)

The Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets of the UHB. It is a core information governance objective that all information assets of the organisation are identified and that the business importance of those assets is established.

There are several IAOs within the UHB, with differing departmental roles. IAOs should work closely with other IAOs and the Information Governance department, which provides support for the SIRO and the Caldicott Guardian, to ensure there is comprehensive asset ownership and clear understanding of responsibilities and accountabilities. This is especially important where information assets are shared by multiple parts of the organisation.

IAOs and the IGCS will support the organisation's SIRO in the overall information risk management function as defined in the Information Risk Management Procedure and associated operational documents. This procedure and the Risk Management Procedure reflect the principles of both the IG Policy and the Risk Management Policy.

The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IAOs will therefore document, understand and monitor:

- What information assets are held, and for what purposes;
- How information is created, amended or added to over time;
- Who has access to the information and why. The UHB IAOs shall receive training from the IGCS to ensure they remain effective in their role as an Information Asset Owner

Aspects of Role	Supporting Actions

Leads and fosters a culture that values, protects and uses information for the success of the organisation and benefit of its patients	• Understands the UHB's plans to achieve and monitor the right NHS IG culture, across the Organisation and with its business partners; • Takes visible steps to support and participate in that plan (including completing own training)
Knows what information an Information Asset holds, and what enters and leaves it and why .i.e. the information flows	• Maintains understanding of 'owned' assets and how they are used up to date; • Documents and reviews information flows • Approves and minimises information transfers while achieving business purposes; • Approves arrangements so that information put onto portable or removable media like laptops and USB Sticks are minimised and are effectively protected to NHS IG standards; • Approves and oversees the disposal mechanisms for information of the asset when no longer needed
Knows who has access to the Information Asset and why, and ensures its use is monitored and compliant with UHB policy and procedures	• Understands the organisation's policy on access to and use of information; • Checks that access provided is the minimum necessary to satisfy business objectives; • Receives records of checks on use and assures self that effective • Checking is conducted regularly
With the support of the IGCS, understands and addresses risks to the asset, and provides assurance to the SIRO via the Information Governance Sub Committee (IGSC)	• Conducts at least annual reviews of information risk in relation to 'owned' assets; • Makes the case where necessary for new investment or action to secure 'owned' assets; • Provides an annual written risk assessment to the IGSC and the SIRO for all assets 'owned' by them
Ensures the asset is fully used for the benefit of the organisation and its patients, including responding to requests for access from others	• Considers whether better use of the information is possible or where information is no longer required; • Receives, logs and controls requests from others for access; • Ensures decisions on access are taken in accordance with the UHB's IG standards of good practice and the policy of the organisation

5. Role: Information Asset Administrator (IAA)

Information Asset Administrators will provide support to their IAO

- Ensure that policies and procedures are followed;
- Recognise potential or actual security incidents;
- Consult their IAO on incident management;
- Ensure that information asset registers are accurate and maintained up to date

6. IAA Tasks

- Ensuring compliance with data sharing agreements within the local area;
- Ensuring information handling procedures are fit for purpose and are properly applied;
- Under the direction of their IAO, ensuring that personal information is not unlawfully exploited
- Recognising new information handling requirements (e.g. a new type of information arises) and that the relevant IAO is consulted over appropriate procedures;
- Recognising potential or actual security incidents and consulting the IAO;
- Reporting to the relevant IAO on current state of local information handling;
- Ensuring that local information handling constraints (e.g. limits on who can have access to the assets) are applied, referring any difficulties to the relevant IAO.
- Act as first port of call for local managers and staff seeking advice on the handling of information;
- Under the direction of their IAO, ensuring that information is securely destroyed when there is no further requirement for it

7. Information Governance

The IAOs will provide assurance to the SIRO and IGSC that :

- Information assets are recorded and included in the organisations asset register and that roles, responsibilities and accountabilities are assigned to the necessary personnel;
- Information Asset Registers are maintained including recording and reviewing of information flows;
- All IA must have a comprehensive library of up to date standard operational procedures that support users and IAAs to carry out their role on a daily basis.

- Robust governance systems, processes and procedures are in place to ensure compliance against local/national requirements including the:
  - Caldicott Principles in Practice (C-PiP) assessment
  - Health and Care Standards (2015) - 3.4 Information Governance and Communications Technology and 3.5 Record keeping
  - IG Toolkit (IGT)
  - Audit

The IG department will support the SIRO in advising and assessing the performance against the required standards.

This procedure must be read in conjunction with related policies/procedures and guidelines.

8. Data Quality

Access to high quality data is essential for good clinical governance and effective performance management. Better information will support the use of best evidence; provide more accurate assessment of the quality of services to support clinical governance, performance management and patient experience.

Each Information asset must have in place:

- Documented local data quality audits (must be undertaken by the IAO/IAA on a regular basis). Audit outcomes to be reported to the relevant group.
- Local data quality issue logs to be implemented and maintained. Common themes to be highlighted to the relevant group for escalation as required.
- User data quality spot checks to be undertaken on a regular basis and the outcomes formally documented.

9. Business Continuity

Business continuity management (BCM) (as defined by the Business Continuity Institute 2001) is:
'*A holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities'.*

BCM is concerned with managing risk to ensure that, at all times, the organisation can continue operating to, at least, a pre-determined minimum level, in the event of a major disruption including major IT system failure/disruption.

It is a requirement of the organisation to ensure that all UHB's IA:

- Have approved Business Continuity (BC) plans in place
- All relevant staff are notified and have received training/guidance on the BC arrangements.
- Regular testing of BC plans to be undertaken with outcomes and lessons learned formally reported to the relevant group/committee

10. Change Control

All changes to IA (e.g. system upgrades) must follow the UHB Change procedure.

11. Information Security

Information Security controls exist in order to safeguard the confidentiality, integrity and availability of all forms of information within the organisation with the overall purpose of protecting personal and corporate information from all threats, whether internal or external, deliberate or accidental. The implementation and monitoring of such controls provides assurance to the Board that comprehensive and consistent information security controls are in place throughout the organisation to ensure business continuity.

It is a requirement of the organisation to ensure that in respect of all IA:

- Information will be protected against unauthorised access.
- Confidentiality of information required through regulatory and legislative requirements will be assured.
- Information will be available to authorised personnel as and when required.
- Regulatory and legislative requirements will be met.
- All breaches of information security, actual or suspected, will be reported and investigated using existing UHB processes.
- All removal media and mobile devices are encrypted to the required standard.
- Regular audits of user access rights are will be undertaken.
- Formal information security risk assessments will be undertaken regularly in order to counter potential threats to UHB IA.

12. Information Risk

Each IAO within the UHB is responsible for risk management and any accreditation programmes of IA under their control. The IAO will be supported

in managing their accreditation processes through contribution from IAA, Information Security Manager, Audit and other relevant staff or contractors.

The IAO must ensure that UHB approved standards are achieved for all IA they own i.e.

- Caldicott Principles in Practice (C-PiP) assessment
- Health and Care Standards (2015) - 3.4 Information Governance and Communications Technology and 3.5 Record keeping
- IG Toolkit (IGT) as far as possible in the Welsh context and
- Audit

The IAO should also consider the IA ongoing accreditation needs in line with the organisations overall risk management and reporting framework.

The IAO must ensure that information risk assessments are performed at least once a quarter on all assets where they have been assigned 'ownership'.

Throughout the operational lifetime of the IA, including post-implementation changes, controls must continue to exist or replaced by ones providing greater effect.

13. Training

The UHB through its training policy will ensure the compliance with the standards as described in related policies/ guidelines:

The IAO and IAA will be required to undertake training as necessary to ensure they remain effective in their role.

All users of the IA to receive appropriate approved training for their role. Training must incorporate data quality, information risk and security, testing of knowledge, and an observation before access is authorised.

Refresher training must be available for all staff that have identified training requirements.

All training will be recorded on the employee staff record using ESR

There will be a documented training plan with aims and objectives to include data quality and information risk/security.

Comprehensive training materials and user guides will be developed and implemented and easily accessible to the user.

14. Audit

The IG department, in conjunction with the Information Security Manager, and Learning and Development department will be assessing compliance against the standards set out in this procedure

IAO and IAA are required to undertake local compliance spot checks/audits to provide assurance to the:

- SIRO
- Chief Operating Officer
- Information Governance Sub Committee,
- Board

The internal audit department will undertake periodic assessments as part of the annual audit programme

The Welsh Audit office will undertake periodic assessments

APPENDIX ONE

Job Title: Senior Information Risk Owner (SIRO)

Purpose of the Job:

The SIRO supported by the IAOs will implement and lead the Information Governance (IG) risk assessment and management processes within the organisation and advise the Board on the effectiveness of information risk management across the organisation.

Specific Responsibilities:

The key roles of the SIRO are to:

- Understand how strategic business goals of the UHB may be impacted by information risks
- Act as an advocate for information risk on the Board
- Take ownership of risk assessment processes for information risk, including the review of the annual information risk assessment
- Review and agree actions in respect of identified information risk
- Ensure that the UHB's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff
- Ensure the Board is adequately briefed on information risk issues
- Undertake strategic information risk management training at least annually

APPENDIX TWO

Job Title: Information Asset Owner (IAO)

Purpose of the Job:
Information Asset Owners are senior individuals involved in running the relevant business.

The IAO's role is to:

- Understand and address risks to the information they 'own'
- Provide assurance to the SIRO on the security and use of these assets

Specific Responsibilities:

- Maintains understanding of 'owned' assets and how they are used
- Approves and minimises information transfers while achieving business purposes
- Approves and oversees the disposal mechanisms for information of the asset when no longer needed
- Knows what information the asset holds and who has access to update the system
- Takes visible steps to ensure compliance to the organisation Information Governance Framework.
- Undertakes regular reviews on the information risk associated with the asset
- Understands and addresses risks to the asset and provides assurance to the SIRO
- Knows who has access and why, and ensures their use is monitored and complain with policy
- Receives, logs and controls requests from other for access
- Ensures that changes to the system are put through a formal 'Request for Change' process with relevant Equality Impact Assessment and Privacy Impact Assessment completed.

APPENDIX THREE

Job Title: Information Asset Administrator (IAA)

Purpose of the Job:
Information Asset Administrators will provide support to their IAO to:

- Ensure that policies and procedures are followed
- Recognise potential or actual security incidents
- Consult their IAO on incident management
- Ensure their information asset registers are accurate and maintained up to date

Specific Responsibilities:

- Ensure compliance with data sharing agreements within the local area
- Ensure information handling procedures are fit for purpose and properly applied
- Under the direction of the IAO, ensure that personal information is not lawfully exploited
- Recognise new information handling requirements and the relevant IAO is consulted over appropriate procedures
- Recognise potential or actual security incidents and consulting the IAO
- Report to the relevant IAO on the current state of asset
- Act as a first port of call for local managers and staff seeking advice on the handling of information

Under the direction of the relevant IAO ensure that information is securely destroyed when there is no further requirement for it (Refer to Records Management Policy and retention and destruction