Reference Number: UHB 287 **Version Number: 1**	**Date of Next Review:** 18 Sep 2018 **Previous Trust/LHB Reference Number: N/A**

Information Risk Management Procedure

Introduction and Aim

This document is written in support of the Information Governance Policy. It should be read alongside the Information Asset Management Procedure and specifically deals with the arrangements for identifying, managing and protecting risks associated with the University Health Board's (UHB's) information assets. The management of risk in the UHB is set out in the Risk Management Policy and this procedure adheres to the general principles of that document and refers to the Risk Assessment and Risk Register Procedure that sets out the UHB's approved methodology.

The successful implementation of this procedure will reduce risk, address business and performance standards, e.g. the requirement to meet Caldicott standards, Health and Care Standards in Wales and the Information Governance Toolkit Standards.

Objectives

The Information Risk Management procedure has 6 key objectives to:

- Set out clear operational arrangements for information risk management in support of the information asset management procedure within the wider UHB risk management framework.
- Support Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) in their operational roles by assigning clear accountability and responsibility documented within their job descriptions for risk management
- Ensure effective governance processes are in place for information assets.
- Provide the required input and reporting to the UHB's risk registers in line with the UHB's Risk Management Policy
- Train staff appropriately
- Provide appropriate and adequate reporting, monitoring and action plans to mitigate and resolve risks

Scope

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

Equality Impact Assessment	An Equality Impact Assessment has been completed for the 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 completed*
Documents to read alongside this Procedure	Information Governance Policy Risk Management Policy Risk Assessment and Risk Register Procedure UHB Corporate Risk and assurance Framework Guide to Incident Reporting Incident Management Investigation and Reporting. [Serious incidents]
Approved by	Information Governance Sub Committee

Accountable Executive or Clinical Board Director	The Senior Information Risk Officer
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	18/09/2015	06/04/2016	New Procedure

Contents Page

1. Introduction

The aim of this procedure is to support managers in the operational delivery of their obligations in respect of the management of risk related to information assets held within the clinical boards and executive directorates. When these obligations are fully met the UHB will be assured that:

- Assets are safe, secure and held in confidence
- Managers have a proactive approach to identified risks and plans in place
- Business continuity is integral to the general approach

2. Purpose

The information risk procedure defines how Cardiff and Vale University Health Board (the UHB) and its delivery partners will manage information risk and how its effectiveness will be assessed. In so doing the procedure supports the organisation's strategic aims and objectives and should enable employees throughout the delivery chain to identify an acceptable level of risk, beyond which escalation of risk management decisions is always necessary. The procedure fits within the organisation's overall corporate risk framework; information risk need not be managed separately from other business risks.

3. Roles and responsibilities

The Senior Information Risk Owner (SIRO) is responsible for developing and implementing the risk management policy and procedures and for reviewing it regularly to ensure that it remains appropriate to the business objectives and the risk environment. The information risk procedure should be published and communicated in a manner that is relevant, accessible and

understandable to all employees and relevant external parties including delivery partners.

Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) in their operational roles have accountability and responsibility documented within their job descriptions for risk management.

4. Information Risk Management

Managing information risks effectively and in line with current guidance and best practice is an important means of enabling the effective use of data for the public benefit.

Managing information risks supports the business strategy and objectives including where the organisation can only influence its delivery partners.

The information risk management structure within the UHB applies specific roles and responsibilities through the SIRO and Caldicott Guardian, the Head of Information Governance and Assurance and the Information Asset Owners (IAOs), Information Asset Administrators (IAAs) and the Information Governance Sub Committee. Appendix A outlines the operational roles and responsibilities of the IAO and IAA in terms of risk management.

The UHB's approach to risk appetite, risk tolerance and the risk assessment methodology is contained in the Risk Management Policy and supported by the Risk Assessment and Risk Register Procedure

The applicable legal and regulatory requirements and the government's minimum mandatory measures and other policies and guidance are to be used in the management of information risk covering physical, procedural, personal and technical measures.

The SIRO has in place escalation and anonymous reporting procedures for risk management decisions.

4. Delivery

The arrangements set out within this procedure are applicable across the UHB and its delivery partners, and contains sufficient detail to ensure consistency across the UHB's full range of business environments and functions.

5. Review & Monitoring

The procedure forms part of the UHB's Information Governance (IG) Controlled Documents Framework. It will be and reviewed routinely every three years by the UHB's Information Governance Sub Committee.

Appendix A. Information Asset Owners ~ Responsibilities and Training

1. 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 Trust. It is a core IG objective that all Information Assets of the organisation are identified and that the business importance of those assets is established.

In the UHB these officers are the clinical board directors and executive directors who act as deputies to the SIRO and provide the SIRO with assurance that all arrangements are in place and obligations are met in terms of information risk.

IAOs should work closely with other IAOs and the Department for Information Governance, Caldicott & SIRO Support (IGCS) 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 UHB's Information Risk Management Policy.

The IAO is expected to understand the overall business goals of the UHB 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.

UHB IAOs shall receive training from the 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 Trust'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	• Maintains understanding of 'owned' assets and how they are used up to date; • 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 Trust 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	• Conducts at least annual reviews of information risk in relation to 'owned' assets;

addresses risks to the asset, and provides assurance to the SIRO via the Information Governance Committee (IGC)	• Makes the case where necessary for new investment or action to secure 'owned' assets; • Provides an annual written risk assessment to the IGC 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 Trust IG standards of good practice and the policy of the organisation

2. 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

3. IAA Tasks

- Maintenance of Information Asset Registers;
- 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

4. Risk Assessment

Key activities are:

- Identify information assets through inventory developed as part of the information asset management procedure.
- Undertake information asset risk assessment
- Undertake a threat analysis
- Identify threats and vulnerabilities and the treatment plan
- Develop and maintain a risk register

The UHB's approach to Risk Management is found in its Risk Management Policy
and Risk Assessment and Risk Register Procedure

5. Assigning Asset Values

In order to identify the appropriate protection for information assets, it is necessary to assess their values in terms of their importance to the organisation or their potential values given certain opportunities. These values are usually expressed in terms of the potential business impacts of unwanted incidents such as loss of confidentiality, integrity and/or availability. This could, in turn, lead to confidential and corporate data losses, loss of public confidence and damage to the UHB image. In order to consistently assess these potential losses and to relate them appropriately, a value scale for information assets should be applied. For each of the information assets and each of the possible losses, i.e. loss of confidentiality, integrity and availability, a value should be assigned.

After assigning values to the information assets it is important that a structured approach to assessing the risk to those assets is used as set out in the Risk Management Policy and Risk Assessment and Risk Register Procedure

6. Identify Threats

Information assets are subject to many kinds of threats. A threat has the potential to cause an unwanted incident which may result in harm to a system or organization and its information assets. This harm can occur from a direct or an indirect attack on an organization's information e.g. its unauthorised destruction, disclosure, modification, corruption, and unavailability or loss. Threats can originate from accidental or deliberate sources or events. A threat would need to exploit vulnerability (see section 7) of the systems, applications or services used by the organization in order to successfully cause harm to the information asset. Examples of threats can be found in Appendix B.

7. Determine the Vulnerabilities

Vulnerabilities are weaknesses associated with an organisation's information assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to these assets. A vulnerability in itself does not cause harm, it is merely a condition or set of conditions that may allow a threat to affect an information asset. Identifying Information Assets, Threats and Vulnerabilities Using the Risk Treatment Plan and examples of vulnerabilities can be found Appendix C.

8. Apply Assessment Methodology

The aim of the risk assessment exercise is to decide for each relevant information asset, what degree of protection is required in terms of confidentiality, integrity and availability. This protection requirement is geared towards the potential loss or damage which could occur in the event of a defined threat occurring. The result is a list of measured risks for each information asset and an assessment of the impact of loss of confidentiality, integrity or availability for that information asset should a perceived threat occur.

The methodology for risk assessment and risk register is found in the UHB's Risk Assessment and Risk Register Procedure

Appendix B: Examples of Threats

Vulnerability / Threat	Potential Impact
Information Asset – Major components	
Failure of one or more of the System components	Loss of service to one or more components which could potentially, depending on the component, lead to full loss of system functionality
Unauthorised physical access to the System component equipment. This includes theft of components, sabotage, misconfiguration etc.)	Theft or damage of systems could lead to unavailability of service, data leakage, breach of confidentiality etc.
Small limited fire, damaging part of the System infrastructure	System computer room still operational but some equipment damaged
Incident causing lack of physical access to System computer room.	No physical access for administration of the System cluster or components
Large fire or other serious incident destroying all Computer room infrastructure and equipment	No access to the system – this would require invocation of a disaster recovery solution (with respect to both the System supplier and the Trust). Potential long term unavailability of the service. The likelihood of a major incident which destroys the entire computer room infrastructure is very low. However, the impact of such an event would be catastrophic.
Information Asset - Networking	
General loss of network connectivity (complete network failure)	Although all servers, workstations and network services may be functioning, the failure of the network means there is no access to Systems. Complete loss of service

Insufficient bandwidth between network components	Loss of service or intolerably slow performance. Certain times of day (e.g. lunchtimes) reduce the performance / accessibility to the System and related components
Electricity failure / fluctuation affects key network components (routers / switches)	Loss of service due to the inability to connect to central servers.
Information Asset - Miscellaneous	
Unavailability of key IT staff for administration / troubleshooting of System issues.	Knowledge of key aspects of the system held by individual members of staff who, if unavailable, couldn't provide support in the event of failure.

Appendix C: Identifying Information Assets, Threats and Vulnerabilities and Using the Risk Treatment Plan,

Identifying Relevant Information Assets

An Information Asset is something to which the UHB directly assigns value and for which it requires protection. The proper management of information assets is vitally important and a key responsibility of the IAOs.

It is important that an inventory of clearly identified information assets is drawn up, ownership identified, components of risk identified and controls to treat the risk put in place. This should be produced by the IAOs for each of their areas and brought together to feed into the UHB's risk assessment and risk register.

Examples of information assets include:

- **Information:** databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements;
- **Paper documents:** contracts, guidelines, company documentation, document containing important business results;
- **Software assets:** application software, system software, development tools and utilities;
- **Physical assets:** computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;
- **People:** personnel, customers, subscribers;
- **Trust image and reputation;**
- **Services:** computing and communications services, other technical services (heating, lighting, power, air-conditioning).

Identify Threats

Examples of threats are:

- **Unauthorised access to, and use of, information, information systems and/or networks and network services**: this normally needs deliberate action to take place, and can result in loss of confidentiality, integrity and/or availability of information, depending on what the unauthorised user is intending to do and the opportunities the user has;
- **Malicious software:** the introduction of malicious software can be deliberate as well as accidental (users implementing "trustworthy" software) which endangers confidentiality, integrity and/or availability;
- **Software failure:** can be a deliberate or accidental event and can result in a loss of integrity and/or availability;
- **Re-routing of messages**: the deliberate re-routing of messages by a third party is a threat which can often take place without the sender even noticing; it could endanger confidentiality, integrity and availability of the message;
- **Unauthorised modification of messages/information:** this is a deliberate threat which can compromise the integrity of the message;
- **Fire:** is a threat which can occur accidentally as well as being caused deliberately, causing loss of availability or integrity (e.g. media affected by heat);
- **Theft:** is a deliberate threat causing loss of confidentiality and/or availability
- **Staff error:** can take place by an accidental or deliberate (sometimes without malicious intent but just because of a lack of awareness) event and can cause a loss of confidentiality, integrity and/or availability.

Determine the Vulnerabilities

Examples of vulnerabilities include:

- **Lack of or inappropriate physical protection:** could, for example, be exploited by theft, hence endangering the confidentiality and availability of information;
- **Wrong selection and use of passwords:** could result in unauthorised access to the information in the system protected by these passwords, hence endangering confidentiality, integrity and/or availability of the information;
- **Unprotected connection to external network (e.g. the Internet):** could lead to the loss of confidentiality, integrity and/or availability of the information stored and processed on the system connected in this way to another

network, which could for example be exploited by theft, hence leading to the loss of confidentiality, availability and/or integrity;

- **Insufficient security training:** could result in users not being aware of security problems which could, for example, endanger confidentiality, or simply in user errors which could cause losses of integrity and/or availability.

Example List of Vulnerabilities

The following lists give examples for vulnerabilities in various security areas, including examples of threats which might exploit these vulnerabilities. The lists can provide help during the assessment of vulnerabilities. It is emphasized that in some cases other threats may also exploit these vulnerabilities.

Personnel Security:

Vulnerability	The vulnerability could be exploited by
Absence of personnel Unsupervised work by outside or cleaning staff Insufficient security training Lack of security awareness Poorly documented software Lack of monitoring mechanisms	Staff shortage Theft Operational support staff error User errors Operational support staff error Use of software in an unauthorised way
Lack of policies for the correct use of telecommunications media and messaging	Use of network facilities in an unauthorized way
Inadequate recruitment procedures	Wilful damage

Physical and Environmental Security:

Vulnerability	The vulnerability could be exploited by
Inadequate or careless use of physical access control to buildings, rooms and offices	Wilful damage
Lack of physical protection for the building, doors, and windows	Theft
Location in an area susceptible to flood	Flooding
Insufficient maintenance/faulty installation of storage media	Maintenance error

Lack of periodic equipment replacement schemes Susceptibility of equipment to humidity, dust, soiling Susceptibility of equipment to temperature variations Susceptibility of equipment to voltage variations	Deterioration of storage media Airborne particles/dust Extremes of temperature Power fluctuation
Unstable power grid	Power fluctuation

Risk Treatment Plan and Information Asset Owners Responsibilities

Having identified the risks to your information asset, it is important that the impacts determined by the threat, vulnerability and asset value are numbered and tabulated using the UHB's Risk Assessment and Risk Register Procedure

From this a Risk Treatment Plan can be developed for each of the discrete risks identified and options considered for their treatment.

The Information Asset Owner's must ensure that:

- Risk assessment is carried out at least annually.
- All Information assets are registered on the Information Asset database.
- All risk assessment controls are implemented
- Regular reports are made to the SIRO and the Information Governance Committee