Trust Policy	NHS Worcestershire Acute Hospitals NHS Trust

Information Risk Policy

Department / Service:	Information Risk
Originator:	Information Governance Manager
Accountable Director:	Chief Finance Officer
Approved by:	Information Governance Steering Group Trust Management Executive
Date of approval:	10th June 2019
First Revision Due:	10th December 2020
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All
Target staff categories	All

Policy Overview:
This policy outlines how Worcestershire Acute Trust will manage information risk to fulfil its duties under the NHS Information Risk Management guidance and how information risk management effectiveness will be assessed and measured.

Latest Amendments to this policy:
Minor update including, relevant dates and approval Appendices removed and available on the Information Governance Webpages 12th June 2020 – Document extended for 6 months whilst in order to have the resource to update and consider any local or national changes to be incorporated.

Contents page:

Appendices - None

Supporting Documents

Supporting Document 1 Equality Impact Assessment
Supporting Document 2 Financial Risk Assessment

Quick Reference Guide

Information Risk

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Trust continuously manages information risk. The aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify and prioritise and manage the risks involved in all Trust activities

Information risk management is an essential element of broader information governance and is an integral part of good management practice

This policy is applicable to all areas of the Trust and adherence should be included in all contracts for outsourced or shared services. There are no exclusions

Below is a brief overview of the areas included within the Information Risk Policy

Senior Information Risk Owner (SIRO)

Named director who has overall responsibility for information risks within the Trust

Information Asset Owner (IAO)

Executives for each directorate / area responsible for identifying and reporting information assets/risks

Information Asset Administrator (IAA)

Operational manager for information systems, reporting to the IAO

Information Governance Manager

Supports SIRO and IAO and ensures that information asset registers are updated centrally. Ensures IG risks are reported in line with national guidelines

Information Security Lead

Leads on all information security risks and cyber incidents

Externally Reportable Incidents

If an information breach is assessed and is deemed to be externally reportable, the IG Manager will seek approval from the SIRO and manage the reporting process

Below is a summary of the elements of Information Risk

- Information Asset Registers
- Information Risk Assessments
- System Level Security Policies
- Monitoring and review of access to information systems
- Information Risk Management Structure
- Information Risk Management Training

1. Introduction

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Trust continuously manages information risk. The aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify and prioritise and manage the risks involved in all Trust activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

The Trust must introduce and embed information risk management into the key controls and approval processes of all major processes and functions of the Trust. This reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff and the Trust itself.

Information risk management is an essential element of broader information governance and is an integral part of good management practice

This policy outlines how Worcestershire Acute Hospitals NHS Trust will manage information risk to fulfil its duties under the Data Security and protection Toolkit and how information risk management effectiveness will be assessed and measured.

This policy will support strategic business aims and objectives and will enable staff to identify an acceptable level of risk, beyond which escalation of risk management is always necessary.

2. Scope of this document

This policy is applicable to all areas of the Trust and adherence should be included in all contracts for outsourced or shared services. There are no exclusions. This policy also includes Cyber security

3. Definitions

IGSG	**Information Governance Steering Group** Forum to discuss / agree all information Governance issues and policies.
PID	**Person Identifiable Data** This is information/data about a person which would enable that person's identity to be established by one means or another. Name and address are very strong identifiers, particularly when available together.
SIRO	**Senior Information Risk Owner** Named director who has overall responsibility for information risks within the Trust
IAO	**Information Asset Owner** Executives for each directorate / area responsible for identifying and reporting information assets/risks
IAA	**Information Asset Administrator** Operational manager for information systems, reporting to the IAO
Risk	Risk is defined as *"the probability or chance that harm from a particular hazard will occur".* The extent of the risk includes the number of people affected, the consequences for them and the impact across the organisation – the level of risk represents the consequences (severity) of harm and the likelihood of it occurring (Ref: Risk Management Strategy)
Consequence	The outcome of an event or situation, expressed qualitatively or quantitatively,

	being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event
Likelihood	A qualitative description or synonym for probability or frequency
Risk Assessment	The overall process of risk analysis and risk evaluation (Ref: Risk Assessment Policy)
Risk Management	The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects (Ref: Risk Management Strategy)
Risk Treatment	When decisions need to be made as to whether the Trust can avoid, reduce, eliminate, accept/retain or transfer the risk - These are usefully described under **the 4 T's** (ref: The Orange Book): The four options are not mutually exclusive and can be used in conjunction with each other. • Tolerate • Terminate • Treat • Transfer (Ref: Risk Management Strategy)
Risk Management Process	The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
Cyber Security	The protection of systems, networks and data in cyberspace.

4. Responsibility and Duties

4.1 Main Responsibilities

The key requirement is for information risks to be managed in a robust way within departments and not be seen as something that is the sole responsibility of another individual or group of individuals. Assurances need to be provided in a consistent manner. To achieve this, a structured approach is needed, building upon the existing information governance framework that is already in place. This structured approach relies upon the identification of information assets and assigning 'ownership' of assets to senior accountable staff known as Information Asset Owners (IAOs).

The aim is to ensure that the approach to information risk management:

- Takes full advantage of existing authority and responsibility structures
- Associates tasks with appropriate management levels
- Avoids unnecessary impacts on day to day business
- Ensures that all the necessary activities are discharged in an efficient, effective, accountable and visible manner
- Is reviewed annually to ensure the process is up to date and includes updated national guidance

4.2 Senior Information Risk Owner (SIRO)

The Trust SIRO is the Chief Finance Officer and takes responsibility for ensuring that information risk is properly identified, managed and that appropriate assurance mechanisms exist.

The SIRO will:

- Ensure that the Trust has departmental Information Asset Owners (IAOs) who understand their roles
- Ensure that information risk assessments are carried out on a bi-annual basis taking account of existing NHS information governance issues
- The SIRO will assess any risks highlighted by the IAO and advise which risks are required to be added to the Trust's risk register
- Ensure that Privacy Impact Assessments are carried out on all new projects when required in accordance with the guidance provided by the Information Commissioner
- Provide periodic reports and briefings to the Accounting Officer and the Trust Board
- Undertake strategic information risk management training at least annually

Detailed guidance for SIROs can be found on the Information Governance Webpages

4.3 Information Asset Owners (IAO)

IAOs are senior individuals responsible for providing assurance that information risks are being managed effectively in respect of the information assets that they 'own'

(see **Information Governance Webpages** for a list of IAO within the Trust)

The IAOs will:

- IAOs must ensure that access to confidential personal information within their area is monitored and audited locally and any breaches are reported on DATIX and investigated. (Confidentiality monitoring audit procedure see the Information Governance Webpages)
- Know what information comprises or is associated with the asset
- Understand the nature and justification of information flows to and from the asset
- Know who has access to the asset and why
- Understand and address risks to the asset
- Ensure that information risk assessments are performed bi-annually providing assurance to the SIRO
- Submit the annual risk assessment results and associated mitigation plans to the SIRO, along with details of any assumptions or external dependencies. Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks
- Forward all completed Information Risk Assessments to the Information Governance Manager who will retain a central register. All risk assessments will be reported to the Information Governance Steering Group. The SIRO will decide which risks should be recorded on the risk register.
- Undertake Privacy Impact Assessments (pre questionnaire questions 1-10) on all new projects when required in accordance with the guidance provided by the Information Commissioner
- Undertake information risk management training at least annually via the IG training tool

Detailed guidance for IAOs can be found on the Information Governance Webpages

4.4 Information Asset Administrators (IAA)

IAA's are operational staff that support IAOs and shall 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.

4.5 Information Governance

The Information Governance Manager will be responsible for supporting the IAO in the identification, delivery and management of an Information Risk Management Programme to address and manage risks to the Trust's Information Assets. They will also hold the Information Asset Register and ensure it is updated centrally. Additional support shall also be provided by the Information Governance Steering Group.

5. Information Risk Management Objectives:

5.1 The objectives of this policy are to:

- Ensure IAO's take action on any risks identified through the risk assessment process and log risks on the Trust's Risk Register where appropriate (The SIRO will agree which risks must be logged and this will be minuted within the Information Governance Steering Group)
- Protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes
- Encourage pro-active rather than re-active risk management
- Provide assistance to and improve the quality of decision making throughout the Trust
- Meet legal or statutory requirements
- Assist in safeguarding the Trust's information assets

5.2 Information Assets

Information assets come in many shapes and forms. Therefore, the following list can only be illustrative. It is generally sensible to group information assets in a logical manner e.g. where they all related to the same information system or business process. Typical assets include:

Personal Information Content
● Databases and data files ● Back-up and archive data ● Audit data ● Paper records (patient case notes and staff records) ● Paper reports
Other Information Content
● Databases and data files ● Back-up and archive data ● Audit data ● Paper records and reports
System/Process Documentation
● System information and documentation ● Operations and support procedures ● Manuals and training materials

● Contracts and agreements ● Business continuity plans
Software
● Applications and System Software ● Data encryption utilities ● Development and Maintenance tools
Hardware
● Computing hardware including PCs, Laptops, PDAs, BlackBerrys and removable media e.g. USB sticks
Miscellaneous
● Environmental services e.g. power and air-conditioning ● People skills and experience ● Shared service including Networks and Printers ● Computer rooms and equipment ● Records libraries

All information assets will be documented within the Trust's Information Asset Register, see Information Governance Webpages for guidance, together with the details of the Information Asset Owner and risk reviews undertaken or planned. These will be updated by the Information Governance Manager.

5.3 Information Risk Management Assessments

A formal information security risk assessment and management programme will be implemented by the Information Governance Manager for all information assets of the Trust to ensure all threats, vulnerabilities and impacts are properly assessed and included within the Trust's risk register.

This requirement also applies to any upgrades or major system amendments to existing systems

For each risk identified an Information Risk Assessment Form (see the Information Governance Webpages) must be completed by the IAO and retained by the Information Governance Manager with the IAO logging the risk on the Trust's Risk Register where appropriate (as defined by the SIRO)

5.4 Information Incident Reporting

All information governance related incidents that occur within the Trust, which may breach security and/or confidentiality of personally identifiable data will be identified, reported and monitored following the Trust's Incident Reporting Process. In line with the NHS England new requirement, any SIRIs (Serious Incidents Requiring Investigation) that are graded as a level 2 are reported using the Incident Reporting Tool within the Information Governance toolkit. This automatically notifies the Department of Health and the Information Commissioner of the incident. See the level 2 incident reporting process on the Information Governance Webpages. These are subsequently published on a quarterly basis on the Incident Reporting Tool and a record of the incident is published on the Trust internet site.

See the Information Governance Webpages for the reporting structure for Cyber Incidents

Following the reporting of a level 2 IGSI a further risk assessment is completed to assess if the Trust should notify the patient / people affected by the incident in the interest of openness or as a legal requirement un the Duty of Candour. See the Information Governance Webpages for the Trusts process for externally reporting Information Governance Incidents

6. Implementation

6.1 Plan for implementation

SIRO will ensure that this policy is sent to all Information Asset Owners (IAO) in order that they can complete assessments and report any risks.
See the Information Governance Webpages for the implementation and monitoring plan

6.2 Dissemination

Copy sent to Information Asset Owners and reference copy available on the intranet.

6.3 Training and awareness

The data security awareness online training is provided by NHS digital via ESR and all staff must completed this training on an annual basis. There is a paper version which reflects the online version provided for ancillary staff.

The Trust's information security risk assessment and management programme will require that the SIRO and IAOs complete the relevant training module:

- Information Risk Management - Introduction
- Information Risk Management - Foundation
- Information Risk Management for SIRO and IAO

This training is available via the Information Governance Team

7. Monitoring and compliance

Please see the monitoring table below:

Page/ Section of Key Document	Key control:	Checks to be carried out to confirm compliance with the policy:	How often the check will be carried out:	Responsible for carrying out the check:	Results of check reported to: *(Responsible for also ensuring actions are developed to address any areas of non-compliance)*	Frequency of reporting:
	WHAT?	**HOW?**	**WHEN?**	**WHO?**	**WHERE?**	**WHEN?**
Page 4 4.1	The Information Risk Management process will be reviewed annually by the Information Governance Manager	IG Manger will ensure national changes are updated	Annually	IG Manager	Take to IGSG annually	Annually
Page 7 5.2	All information assets will be documented within the Trust's Information Asset Register, together with the details of the Information Asset Owner and risk reviews undertaken or planned.	Initial assessment completed in 2012 and IAO to update with new systems/assets	Annually	IG manager	Annual update to IGSG	Annually
Page 5 4.3	Ensure that information risk assessments are performed annually providing assurance to the SIRO	Risk Assessment to be carries out by IAO	Annually	IAO	Risk assessment sent to Information Governance Manager to be reviewed. High risks to be presented at the IG steering group for the attention of the SIRO	Bi-annually
Page 6 5.1	The SIRO will agree which risks must be logged and this will be minuted within the Information Governance Steering Group)	IG manager will ensure risk reports are taken to the IGSG and SIRO will take further if necessary	As necessary	IG manager/SIRO	IGSG	As necessary

8. Policy Review

This policy will be reviewed biannually by the Information Governance Manager and relevant key staff from the Information Governance team, Information Security and the members of the Information Governance Steering Group.

9. References:

References:	Code:
Information Governance Policy	WAHT-CG-579
Corporate Records Management Policy	WAHT-CG-127
Code of Conduct for Employees in Respect of Confidentiality	WAHT-IG-001
Safe Haven Policy	WAHT-CG-128
Risk Management Strategy	WAHT-CG-007
Risk Assessment Procedure	WAHT-CG-002
Incident reporting policy	WAHT-CG-008
ICT Policy	WHITS-ICT-002

10. Background

10.1 Equality requirements

- No impact from the equality assessment (Supporting Document 1)

10.2 Financial risk assessment

- No impact from the financial risk assessment (Supporting Document 2)

10.3 Consultation

- The policy has been created by the Information Governance Manager with input from the Information Governance Steering Group.

10.4 Approval process

- This policy will be approved at the Information Governance Steering. Minor changes can be approved by the SIRO via the IGSG prior to the 2 year review.

10.5 Version Control

- This section should contain a list of key amendments made to this document each time it is reviewed.

Date	Amendment	By:
Sept 2012	Document created	Information Governance Manager
Sept 2014	General update into latest policy template and minor amendments to content (Version 3)	Information Governance Manager
Jan 2017	Updated specified years (2014/2016) to cover current policy approval Inclusion of Cyber Security Breach Reporting Inclusion of process for externally reportable incidents Update of Information Asset Owners	Information Governance Manager
May 2019	Minor update including, relevant dates and approval Appendices removed and available on the Information Governance Webpages	Information Governance Manager

Supporting Document 1 - Equality Impact Assessment Tool

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

		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	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
5.	**If so can the impact be avoided?**	No	
6.	**What alternatives are there to achieving the policy/guidance without the impact?**	No	
7.	**Can we reduce the impact by taking different action?**	No	

If you have identified a potential discriminatory impact of this key document, please refer it to Assistant Manager of Human Resources, 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 Assistant Manager of Human Resources.

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author and attached to key document when submitted to the appropriate committee for consideration and approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	None

If the response to any of the above is yes, please complete a business case and which is signed by your Finance Manager and Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval