Information Risk Policy

Department / Service:	Information Governance
Originator:	Information Governance Manager
Accountable Director:	Senior Information Risk Owner (Board Member)
Approved by:	Information Governance Steering Group
Date of approval:	24th April 2023
Review Date: **This is the most current document and should be used until a revised version is in place**	24th April 2026
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All
Target staff categories	All

Policy Overview:

This policy outlines how Worcestershire Acute Hospitals Trust will manage information risk to fulfil its duties on information risk management and how its effectiveness will be assessed and measured.

Key amendments to this document

Date	Amendment	Approved by:
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.	
23rd Dec 2020	Document extended for 3 months until March 2021 due to urgent COVID work	Approved by Rebecca Brown
31st March 2021	Document extended for 6 months as per Trust agreement 11.02.2021	
16th July 2021	Document review date amended as per the Key Documents policy 3 year approval update.	
12th April 2022	Document extended to the end of September to allow for thorough review	Annie Osborne-Wylde/ Rebecca Brown
April 2023	General updates: • Data Protection terminology • SIAO role explained • General updated around roles and training (version 5)	Information Governance Manager

Contents page:

Appendices

Supporting Documents

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, 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 adherance should be included in all contracts for out sourced and shared services. There are no exclusions

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

Senior Information Risk Owner (SIRO)
A named director who has overall responsibility for information risk within the Trust

Senior Information Asset Owner (SIAO)
Director of Operation for clinical divisions and Deputy SIRO for corporate areas, responsible for identifying and reporting information risks to the SIRO

Information Asset Owners/ Administrators (IAO/A)
Operational managers or systems admin, reporting to the SIAOs

Information Governance Manager
Supports the SIRO and SIAOs d ensures that Data Protection breaches are reported in line with national guidelines

Data Protection Officer (DPO)
The DPO ensures that the Trust processes the personal data of its staff, patients, providers or any other individuals (also referred to as data subjects) in compliance with data protection rules.

Information Security Lead
Leads on all information security risks and cyber incidents

Below is a summary of the elements of Information Risk

- Data Mapping and the collection of information on data that the Trust processes
- Information Asset Registers
- Data Protection Impact Assessments/Risk Assessments
- Information Risk Management Training
- Monitoring and review of access to Trust information systems
- Information Risk Management structure

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, 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.
PII	**Person Identifiable Information** 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
SIAO	**Senior Information Asset Owner** Executives for each directorate / area responsible for identifying and reporting information assets/risks
IAO	**Information Asset Owner** Department/system managers responsible for identifying and reporting information assets/risks
IAA	**Information Asset Administrator** Operational manager for information systems, reporting to the SIAO/IAO
DPO	**Data Protection Officer** Ensures that the Trust processes the personal data of its staff, patients, providers or any other individuals (also referred to as data subjects) in compliance with data protection rules.

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	Cyber security is how individuals and organisations reduce the risk of cyber-attack. Cyber security's core function is to protect the devices and the services staff access - both online and at work - from theft or damage.

4. Responsibility and Duties

4.1 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 Senior Information Asset Owners (SIAOs).

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 has responsibility for ensuring that information risk is properly identified, managed and that appropriate assurance mechanisms exist. The SIRO is a member of the Board and has delegated responsibility from the Chief Executive.

The SIRO will:

- Ensure that the Trust has Divisional Senior Information Asset Owners (SIAOs) who understand their roles
- The SIRO will assess any risks highlighted by the SIAO and advise which risks are required to be added to the Trust's risk register
- Ensure that Data Protection Impact Assessments (DPIA) are carried out for all new systems or suppliers, when required in accordance with the guidance provided by the Information Commissioner
- Provide periodic reports and briefings to the Trust Board
- Undertake strategic information risk management training

4.3 Senior Information Asset Owners (SIAO)

SIAOs are senior individuals responsible for providing assurance to the SIRO that information risks are being managed effectively in respect of the information assets that they 'own'. All Divisional Directors of Operations within the 5 clinical divisions are SIAOs plus a single SIAO covering the corporate divisions. The SIRO has delegated responsibility to the SIAOs

4.4 Information Asset Owners (IAO)

Information Asset Owners (IAOs) are individuals involved in running the relevant business. Their role is to understand what information is processed; i.e. held, added, removed, how information is moved and who has access and why. As a result, they are able to understand and address risks to the information assets they 'own' and to provide assurance to the SIAO on the security and use of the assets. In larger organisations, an IAO might be a department head, for example. The SIAOs have delegated responsibility to the IAOs.

4.5 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.

4.6 Information Governance

The Information Governance Manager will be responsible for supporting the SIAO 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.

Information Governance manages a rolling program of data mapping, including risk assessments, and these are signed off by the SIAO and reported to IGSG.

4.7 Data Protection Officer (DPO)

The DPO ensures that the Trust processes the personal data of its staff, patients, providers or any other individuals (also referred to as data subjects) in compliance with data protection rules.

5. Information Risk Management Objectives:

5.1 The objectives of this policy are to:

- Ensure SIAO's take action on any risks identified 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 Management of 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, 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 Programme

A formal information risk 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. The programme includes information asset management, derived from data mapping and information risk assessments

5.4 Information Incident Reporting

All Data Protection related incidents that occur within the Trust, which meet the criteria for external reporting are reported by the Information Governance Manager once approved by the SIRO

They are reported on the Data Security and Protection Toolkit which includes a tool for reporting data security incidents to the Information Commissioner's Office, the Department of Health and Social Care and NHS England.

Organisations must notify a breach of personal data within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also inform those individuals without undue delay.

6. Implementation

6.1 Plan for implementation

SIRO will ensure that this policy is sent directly to all Senior Information Asset Owners (SIAO) and published on the Trusts Key Policy page

6.2 Dissemination

SIAO to ensure that this policy is disseminated to all of their department managers and managers of information assets.

6.3 Training and awareness

The Data Security Awareness online training is provided by NHS Digital via ESR and all staff must have completed this training on an annual basis.

Specialist risk training will be provided to support the roles of the SIRO, SIAO and IAO.

7. Monitoring and compliance

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?**
4.2	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
4.6	All risk associated with the information risk programme will be reported to the SIRO	Via IGSG reports or direct reporting from SIAOs	As necessary	IG Manager	IGSG	As necessary

8. Policy Review

This policy will be updated every two years by the Information Governance Manager and approved by the Information Governance Steering Group to reflect the Trust's development of policies and procedures and the changing needs of the NHS or when necessary following changes to the law.

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
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.

Contribution List

This key document has been circulated to the following individuals for consultation.

Designation
Members of the Information Governance Steering Group, who include: SIRO, DPO, Caldicott Guardians, SIAO

This key document has been circulated to the following individuals for consultation.

Committee
Information Governance Steering Group

10.4 Approval Process

This policy will be approved at the Information Governance Steering Group and an update will be sent on to Trust Management Executive (TME).

10.5 Version Control

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
2020	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. 23rd Dec 2020 - Document extended for 3 months until March 2021 due to urgent COVID work – Approved by Rebecca Brown 31st March 2021- Document extended for 6 months as per Trust agreement 11.02.2021 16th July 2021- Document review date amended as per the Key Documents policy 3-year approval update. 12th April 2022- Document extended to the end of September 2022	Deputy SIRO
April 2023	General updates: • Data Protection terminology • SIAO role explained • General updated around roles and training (version 5)	Information Governance Manager

Supporting Document 1 – Equality Impact Assessment form

To be completed by the key document author and included as an appendix to key document when submitted to the appropriate committee for consideration and approval.

Please complete assessment form on next page;

NHS Worcestershire Acute Hospitals NHS Trust

Herefordshire and Worcestershire Safe and effective health and care services

Herefordshire & Worcestershire STP - Equality Impact Assessment (EIA) Form
Please read EIA guidelines when completing this form

Section 1 - Name of Organisation (please tick)

Herefordshire & Worcestershire STP		Herefordshire Council		Herefordshire CCG	
Worcestershire Acute Hospitals NHS Trust		Worcestershire County Council		Worcestershire CCGs	
Worcestershire Health and Care NHS Trust	☒	Wye Valley NHS Trust		Other (please state)	

Name of Lead for Activity	

Details of individuals completing this assessment	**Name**	**Job title**	**e-mail contact**
	Annie Osborne-Wylde	**IG Manager**	**Annie.osborne-wylde@nhs.net**
Date assessment completed	**24th April 2023**		

Section 2

Activity being assessed (e.g. policy/procedure, document, service redesign, policy, strategy etc.)	**Title:** Information Risk Policy			
What is the aim, purpose and/or intended outcomes of this Activity?	Policy document to inform staff.			
Who will be affected by the development & implementation of this activity?	□ □ □ □	Service User Patient Carers Visitors	x □ □ □	Staff Communities Other ______________________
Is this:	X Review of an existing activity □ New activity □ Planning to withdraw or reduce a service, activity or presence?			

What information and evidence have you reviewed to help inform this assessment? (Please name sources, eg demographic information for patients / services / staff groups affected, complaints etc.	National guidelines
Summary of engagement or consultation undertaken (e.g. who and how have you engaged with, or why do you believe this is not required)	WAHT Information Governance Steering Group
Summary of relevant findings	Approved

Section 3

Please consider the potential impact of this activity (during development & implementation) on each of the equality groups outlined below. **Please tick one or more impact box below for each Equality Group and explain your rationale**. Please note it is possible for the potential impact to be both positive and negative within the same equality group and this should be recorded. Remember to consider the impact on e.g. staff, public, patients, carers etc. in these equality groups.

Equality Group	**Potential positive impact**	**Potential neutral impact**	**Potential negative impact**	**Please explain your reasons for any potential positive, neutral or negative impact identified**
Age		x		
Disability		x		
Gender Reassignment		x		
Marriage & Civil Partnerships		x		
Pregnancy & Maternity		x		
Race including Traveling Communities		x		
Religion & Belief		x		
Sex		x		
Sexual Orientation		x		
Other Vulnerable and		x		

Equality Group	Potential <u>positive</u> impact	Potential <u>neutral</u> impact	Potential <u>negative</u> impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Disadvantaged Groups (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling communities etc.)				
Health Inequalities (any preventable, unfair & unjust differences in health status between groups, populations or individuals that arise from the unequal distribution of social, environmental & economic conditions within societies)		x		

<u>Section 4</u>

What actions will you take to mitigate any potential negative impacts?	Risk identified	Actions required to reduce / eliminate negative impact	Who will lead on the action?	Timeframe
	N/A	.		
How will you monitor these actions?				
When will you review this EIA? (e.g. in a service redesign, this EIA should be revisited regularly throughout the design & implementation)				

<u>Section 5</u> - Please read and agree to the following Equality Statement

1. Equality Statement

1.1. All public bodies have a statutory duty under the Equality Act 2010 to set out arrangements to assess and consult on how their policies and functions impact on the 9 protected characteristics: Age; Disability; Gender Reassignment; Marriage & Civil Partnership; Pregnancy & Maternity; Race; Religion & Belief; Sex; Sexual Orientation

1.2. Our Organisations will challenge discrimination, promote equality, respect human rights, and aims to design and implement services, policies and measures that meet the diverse needs of our service, and population, ensuring that none are placed at a disadvantage over others.

1.3. All staff are expected to deliver services and provide services and care in a manner which respects the individuality of service users, patients, carer's etc, and as such treat them and members of the workforce respectfully, paying due regard to the 9 protected characteristics.

Signature of person completing EIA	
Date signed	24th April 2024
Comments:	
Signature of person the Leader Person for this activity	
Date signed	
Comments:	

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:	

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