

Corporate Records Management Policy

Department / Service:	Corporate
Originator:	Information Governance Manager
Accountable Director:	Chief Finance Officer/Chief Digital Officer (SIRO)
Approved by:	Information Governance Steering Group, TME
Date of approval:	17 th October 2022
Review Date:	16 th October 2026
This is the most current document and is to be used until a revised version is in place	
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	All Staff
Target staff categories	All Staff

Policy Overview:

This policy defines a structure for Worcestershire Acute Hospitals Trust to ensure records are maintained, managed and controlled effectively and at best value, commensurate with legal, operational and information needs. This policy is designed to provide all professionals working within the Trust with information on the principles of good documentation and record keeping within their administrative and clinical practice and ensure consistent standards across professional groups.

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 December 2020	Document extended for 3 months until March 2021 due to urgent COVID	Rebecca Brown
31st March 2021	Document extended for 6 months as per Trust agreement 11.02.2021	
16 th July 2021	Document review date amended as per the Key Documents policy 3 year approval update.	Trust policy
12th April 2022	Document extended to the end of September to allow for thorough review	Annie Osborne-Wylde and Rebecca Brown
Sept 2022	Re-write in line with national guidance update 2021	IGSG/TME
22 nd October 2025	Document extended for 6 months to allow time to ensure that all updates are included	Matthew Thurland
16 th April 2026	Document extended for 6 months to allow time for review and update	Matthew Thurland

Contents page:

Quick Reference Guide

1. Introduction
2. Scope of this document
3. Definitions
4. Responsibility and Duties
5. Policy detail
6. Implementation of key document
 - 6.1 Plan for implementation
 - 6.2 Dissemination
 - 6.3 Training and awareness
7. Monitoring and compliance
8. Policy review
9. References
10. Background
 - 10.1 Equality requirements
 - 10.2 Financial Risk Assessment
 - 10.3 Consultation Process
 - 10.4 Approval Process
 - 10.5 Version Control

Appendices

Appendix 1

Supporting Documents

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

1. Introduction

1.1 Worcestershire Acute Hospitals NHS Trust is dependent on its records to operate efficiently and to account for its actions. This policy defines a structure for the Trust to ensure adequate records are maintained, managed and controlled effectively and at best value, commensurate with legal, operational and information needs. This policy is designed to provide all staff working within the Trust with information on the principles of good documentation and record keeping within their administrative and clinical practice and ensure consistent standards across professional groups.

1.2 Our organisation's records are our corporate memory, providing evidence of actions and decisions and representing a vital asset to support our daily functions and operations. They support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public who have dealings with us. They support consistency, continuity and efficiency and productivity and help us deliver our services in consistent and equitable ways.

1.3 All health and care employees are responsible for managing records appropriately. Records must be managed in accordance with the law. Health and care professionals also have professional responsibilities, for example, complying with the Caldicott Principles and records keeping standards set out by registrant bodies.

1.4 Public Records Act 1958

[The Public Records Act 1958](#) is the principal legislation relating to public records. Records of NHS organisations are public records in accordance with Schedule 1 of the Act. This means that employees are responsible for any records that they create or use in the course of their duties. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. The Act applies regardless of the format of the records. The Secretary of State for Health and Social Care and all NHS organisations have a duty under the Act to make arrangements for the safekeeping and eventual disposal of all types of records. This is carried out under the overall guidance and supervision of the Keeper of Public Records who reports annually on this to the Secretary of State for Culture, Media and Sport who is accountable to parliament. [The NHS Standard Contract](#) notes a contractual requirement on organisations which are not bound by either the Public Records Act 1958

1.5 Freedom of Information Act 2000

[The Freedom of Information Act \(FOIA\)](#) governs access to and management of non-personal public records. The FOIA was designed to create transparency in government and allow any citizen to know about the provision of public services through the right to submit a request for information. This right is only as good as the ability of those organisations to supply information through good records management programmes. Records managers should adhere to the [code of practice on record keeping](#) issued by the Secretary of State for Culture, Media and Sport, under section 46 of the FOIA. The section 46 Code of Practice is used as a statutory statement of good practice by the regulator and the courts.

1.6 UK GDPR and Data Protection Act 2018.

The UK GDPR is the principal legislation governing how records, information and personal data are managed. It sets in law how personal and special categories of information may be processed. The Data Protection Act 2018 [principles](#) are also relevant to the management of records. Under the UK GDPR, organisations may be required to undertake Data Protection

Impact Assessments (DPIA) as set out in Section 3 of this Records Management Code. The UK GDPR also introduces a principle of accountability. The Information Commissioner's Office (ICO) [Accountability Framework](#) can support organisations with their obligations. Good records management will help organisations to demonstrate compliance with this principle.

1.7 Health and Social Care Act 2008

Regulation 17 under the Health and Social Care Act 2008 requires that health and care providers must securely maintain accurate, complete and detailed records for patients or service users, employment of staff and overall management. The CQC are responsible for regulating this and have issued [guidance](#) on regulation 17. The CQC may have regard to the Code when assessing providers' compliance with this regulation.

1.8 The Records Management Code of Practice for Health and Social Care 2021 (from this point onwards referred to as the Code) is a guide for organisations to use in relation to the practice of managing records. This guide replaces the 2006/2009 and 2016 versions. It is relevant to organisations working within, or under contract to, the NHS in England. The Code also applies to adult social care and public health functions commissioned or delivered by local authorities. The Code provides a framework for consistent and effective records management based on established standards. It includes guidelines on topics such as legal, professional, organisational and individual responsibilities when managing records. It also advises on how to design and implement a records management system including advice on organising, storing, retaining and deleting records. It applies to all records regardless of the media they are held on. The guidelines in this Code draw on published guidance from The National Archives and best practice in the public and private sectors. It is informed by lessons learnt and it will help organisations to implement the recommendations of the [Mid Staffordshire NHS Foundation Trust Public Inquiry](#) relating to records management and transparency.

Standards and practice covered by the Code will change over time so it will be reviewed and updated as necessary. In particular, it should be noted that at the time of writing there are a number of on-going public inquiries including the Independent Inquiry into Historic Child Sex Abuse (IICSA) and Infected Blood Public Inquiry (IBI). This means that records must not be destroyed until guidance is issued by the inquiry. Future public inquiries may lead to specific records management requirements. Where that happens, the Inquiry will publish additional guidance on its website. NHS England and Improvement may also issue guidance to the health and care system relating to the inquiry.

2. Scope of this document

2.1 This policy refers to all operational records

The ISO standard [ISO 15489-1:2016](#) defines a record as:

- Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business

[Section 205](#) of the Data Protection Act 2018 defines a health record as a record which:

- consists of data concerning health
- has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.

2.2 The guidelines in this Code apply to NHS and adult social care records. This includes:

- records of patients treated by NHS organisations
- records of patients treated on behalf of the NHS in the private healthcare sector
- records of private patients treated on NHS premises
- records created by providers contracted to deliver NHS services (for example, GP services)
- adult service user records who receive social care support
- jointly held records
- records held as part of a Shared Care Records programme
- records held by local authorities such as public health records, contraceptive and sexual health service records
- staff records
- complaints records
- corporate records – administrative records relating to all functions of the organisation

2.3 The guidelines apply regardless of the media on which the records are held. Usually these records will be on paper or digital. However, some specialties will include physical records, such as physical moulds made from plaster of Paris. Examples of records that should be managed using the guidelines in this Code include:

- health and care records
- registers - for example, birth, death, Accident and Emergency, theatre, minor operations
- administrative records, for example, personnel, estates, financial and accounting records, notes associated with complaint-handling
- x-ray and imaging reports, output and images
- secondary uses records (such as records that relate to uses beyond individual care), for example, records used for service management, planning, research

2.4 Examples of record formats that should be managed using the guidelines from this code:

- Digital
- Paper
- Photographs, slides, and other images
- Microform (microfiche or microfilm)
- Physical records (records made of physical material such as plaster, gypsum and alginate moulds)
- Audio and video tapes, cassettes, CD-ROM etc
- e-mails
- Computerised records
- Scanned records
- Text messages (SMS) and social media (both outgoing from the NHS and incoming responses from the patient or service user) such as Twitter and Skype
- Metadata added to, or automatically created by, digital systems when in use. Content can sometimes be of little value if it is not accompanied by relevant metadata
- Websites and intranet sites that provide key information to patients or service users and staff

3. Definitions

Records	Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuance of legal obligations or in the transaction of business
Records	The above definition and qualities apply regardless of the record's format whether it is a sheet of paper, email, photograph or database entry. The retention of emails as records is a particular challenge.
Records Life Cycle	The records lifecycle, or the information lifecycle, is a term that describes a controlled regime in which information is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest
Records Management	A discipline which utilises an administrative system to direct or control the creation, version control, distribution, filing, retention, storage and disposal of records. This is done in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record. The key components of Records Management are:
Records Management System	A records management system should cover each stage of the lifecycle: <ul style="list-style-type: none"> • creation: create and log quality information • using: use or handle • retention: keep or maintain in line with NHS recommended retention schedule • appraisal: determine whether records are worthy of archival preservation • disposal: dispose appropriately according to policy
Appraisal	Refers to the process of determining whether records are worthy of permanent archival preservation.
Metadata	Metadata within the structure of a record, makes it easier to manage or find information, be it in the form of webpages, electronic documents, paper files or databases and for metadata to be effective, it needs to be structured and consistent across organisations

4. Responsibility and Duties

Records management is recognised as a specific corporate responsibility within every organisation. It should provide a managerial focus for records of all types, in all formats throughout their lifecycle, from creation through to ultimate disposal.

4.1 Statutory Requirements

The Secretary of State for Digital, Culture, Media and Sport sets out the requirement for all public bodies to have a records management code of practice ([section 46\(6\) of the Freedom of Information Act 2000](#))

4.2 Managerial Accountability and Responsibility

The Chief Executive has overall accountability for the management of records within the Trust.

As records management activities are undertaken throughout the organisation, mechanisms must be in place to enable the Senior Information Asset Owners to exercise an appropriate level of management of this activity.

All departmental managers are responsible for regular, localised monitoring of the quality of documentation and adherence to this policy. In particular, managers and senior clerical staff should annually undertake an audit of the records for which they are responsible to ensure that the standards, as detailed in this policy, are maintained.

All staff, whether working with clinical or administrative records, must be appropriately trained so that they are competent to carry out their designated duties and fully aware of their personal responsibilities in respect of record keeping and records management. The Information Governance Manager will ensure a Corporate Records Audit is included in the team work programme.

4.3 Professional Obligations

Staff who are registered to a Professional body, such as the General Medical Council (GMC), Nursing and Midwifery Council (NMC) or Social Work England will be required to adhere to record keeping standards defined by their registrant body. This is designed to guard against professional misconduct and to provide high quality care in line with the requirements of professional bodies.

The Academy of Medical Royal Colleges (AoMRC) [generic medical record keeping standards](#) were prepared for use in the NHS, primarily in acute settings but the standards are useful for all health and care settings. The AoMRC notes that a medical record, whether paper or digital, must adhere to certain record keeping standards. The Royal College of Nursing has produced [guidance on abbreviations and other short forms in patient or client records](#). Further information about professional standards for records can be obtained from your relevant professional body.

5. Records Management Policy Detail

A systematic and planned approach to the management of records within the organisation, from the moment they are created to their ultimate disposal, ensures that the organisation can control both the quality and the quantity of the information that it generates: it can maintain the information in a manner that effectively services its needs, those of government and of the citizen: and it can dispose of the information efficiently when it is no longer required. This applies to all records whether manual or computerised records.

Records are valuable because of the information they contain and that information is only usable if it is correctly and legibly recorded in the first place, is then kept up to date, and is easily accessible when needed. Good record keeping ensures that:

- Employees work with maximum efficiency without having to waste time hunting for information.
- There is an 'audit trail', which enables any record entry to be traced to a named individual at a given date/time with the secure knowledge that all alterations can be similarly traced.
- New staff can see what has been done, or not done, and why.
- Any decisions made can be justified or reconsidered at a later date.
- Good records management is essential for:
 - Providing high quality patient care
 - Effective communication and dissemination of information between members of multi-disciplinary health care teams

- An accurate account of continuous assessment, treatment, and evaluation reflected in a care plan
- The ability to detect problems, such as changes in the patient's or client's condition, at an early stage
- Corporate memory
- Clinical liability
- Historical purposes
- Purchasing and contract service agreement management
- Financial accountability
- Disputes or legal action
- Continuity of care

It is therefore important to ensure:

- Important and relevant information is recorded and completed
- It is legible, written in black ink, and can be easily read and reproduced when required
- Information/records are easily accessible and kept up-to-date
- Information is shared rather than copied in order to reduce risks to confidentiality
- Records are disposed of as soon as possible subject to national (Records Management Code of Practice for Health and Social Care 2021) or locally determined retention periods. See Information Governance Webpages for further details
- Records are shredded or disposed of via the Trust's contracts for disposal of confidential waste

What needs to be done to achieve best standards?

- Managers in all work units need to ensure that staff are aware of the current rules on such issues as Data Protection and access to patient information.
- Managers should ensure that staff are suitably trained in record keeping, security and storage of information/records (manual and computerised.)

Records may be required as evidence:

- Before a court of law
- In order to investigate a complaint at a local level
- By Professional Conduct Committees e.g. NMC, which considers complaints about professional misconduct

The main objectives of this policy are:

5.1 Accountability – that adequate records are maintained to account fully and transparently for all actions and decisions in particular:

- To protect legal and other rights of staff or those affected by these actions
- To facilitate audit or examination
- To provide credible and authoritative evidence

Quality – that records are complete and accurate and the information they contain is reliable and its authenticity can be guaranteed

Please see the additional guidance documents (Organising Records Guidance [available on this link](#)) for best practice for:

- Designing a record keeping system
- Conducting a DPIA for new record keeping systems

- Declaring a record
- Organising records
- Using metadata to organise and find records
- Applying security classifications

Please see the additional guidance documents (Records storage for operational use guidance [available on this link](#)) for best practice for:

- Management and storage of paper records
- Management and storage of digital records
- Managing Offsite records

Accessibility – those with a legitimate right of access can efficiently retrieve the information within them, for as long as the records are held by the Acute Trust.

Security – that records will be secure from unauthorised or inadvertent alteration or erasure, that access and disclosure will be properly controlled, and audit trails will track all use and changes. Records will be held in a robust format, which remains readable for as long as records are required

Retention and disposal – that there are consistent and documented retention and disposal procedures to include provision for permanent reservation of archival records

Please see the separate Corporate Records Management Retention Schedule for full details of specific retention periods

Please see the additional guidance documents (Retention Management Guidance [available on this link](#)) for best practice for:

- Management of records when the minimum retention period is reached
- Appraisal of records
- Destroying and deleting records
- Continued retention
- Records for permanent preservation

Performance measurement – that the application of records management procedures are regularly monitored against agreed indicators and action taken to improve standards as necessary.

5.2 Records Management - Scanning

For reasons of business efficiency or in order to address problems with storage space, NHS organisations may consider the option of scanning into electronic format records which exist in paper format. Where this is proposed, the factors to be taken into account include:

The costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept;

The need to consult in advance with the local Place of Deposit or The National Archives (TNA) with regard to records which may have archival value, as the value may include the format in which it was created; and

The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the Code of Practice for the Implementation of BS 10008 - Evidential Weight and Legal Admissibility of Information Stored Electronically

In order to fully realise the benefits of reduced storage requirements and business efficiency, organisations should consider disposing of paper records that have been copied into electronic format and stored in accordance with the appropriate standards.

Code of Practice for the Implementation of BS 10008 - Evidential Weight and Legal Admissibility of Information Stored Electronically.

The issue of Legal Admissibility is at the core of records management principles. An organisation must be able to prove (to a court of law or some other statutory body) that the contents of a particular document or data file created or existing within an Electronic Document Management System have not changed since the time of storage. If the data file is an electronically stored image of an original paper document, an organisation must be able to prove that the electronic image is a true representation of the original. Proving the authenticity of electronically stored documents is crucial to their admissibility in a court.

It is important for the system to be able to produce output that will ensure that a document is appropriately authenticated. The Code insists that the procedures and processes be audited annually, or more frequently for legally sensitive archives, to make sure that the approved procedures are being observed or that new ones meet the requirements of the Code and are formally and properly incorporated in the manual

5.3 Confidentiality and Security of Records

All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty of confidentiality. Everyone working for or with the NHS who records, handles, stores or otherwise accesses patient information has a personal common law duty of confidence to patients/colleagues and to their employer. This duty of confidence continues after the death of the patient or after an employee or contractor has left the NHS. Trust staff are advised of their responsibilities on commencement of their employment and is reflected in their contracts.

Through the Caldicott Guardian, Information Security and Information Governance Leads, the Trust must also ensure that information is shared “on a need to know” basis and that it is continuously improving confidentiality and security procedures governing access to and storage of clinical information.

Managers must ensure that all staff are made aware of their responsibilities regarding confidentiality and security of records by completing Data Security Awareness Mandatory training.

5.4 Electronic Records

Electronic information is subject to the same principles as paper records. For administrative records (e.g. minutes of meetings) these must comply with the principles laid out in this policy to aid effective storage and retrieval for responding to queries under the Freedom of Information Act.

Emails should be regarded as a transitory means of communication. Any information transmitted by email which falls into a category shown in the retention schedule should be absorbed into a mainstream filing system which is subject to the requirements laid out in section 5 “Record Keeping Standards”.

As an example a Word attachment containing minutes of a meeting should be stored in either the electronic or manual filing system of the person sending the email. Neither the sender nor recipient should save the email, with the attachment, in perpetuity. For this same reason any

information sent by email which is intended to have some permanence should be transmitted as a file attachment and is subject to the above conditions.

5.5 Electronic Records Freedom of Information Act 2000 (FOI)

- The Freedom of Information Act was passed on 30th November 2000 and is part of the Government's commitment to greater openness in the public sector.
- On 1st January 2005, the Act gave a general right of access to all types of 'recorded information' held by public authorities, subject to certain conditions and exemptions contained in the Act.
- Simply, any person of any nationality, who makes a request to a public authority for information, must be informed whether the public authority holds the information and if so, that information must be supplied. This is referred to as the 'duty to confirm or deny'.

5.6 FOI Publication Scheme

- In addition to providing information when asked to do so, the Act also requires public authorities to be proactive in the release of official information.
- As a result, by 31st October 2003, every public authority was required to adopt and maintain a publication scheme setting out how it intends to publish the different classes of information it holds, and whether there is to be a charge for the information disclosed. The trust's FOI publication scheme is regularly updated and has been approved by the Information Commissioner.
- The Trust's FOI Publication Scheme can be found on the Trusts internet site.
- Freedom of Information Act 2000 Policy
- The trust's FOI Act 2000 Policy provides a framework within which the trust will ensure compliance with the requirements of the Act. It is not a statement of how compliance will be achieved; this will be a matter for operational procedures.
- The Policy will underpin any operational procedures and activities connected with the implementation of the Act.
- The FOI Act 2000 Policy applies to all trust employees and to non-executive directors.
- The Freedom of Information Act does not overturn the common law duties of confidence nor does it overturn the requirements of the Data Protection Act 1998.

5.7 Further details from the NHSX Code of Practice can be found in the separate Corporate Records Management Retention Schedule. This document includes:

- Part 1: Public and Statutory Inquiries
- Part 2: Retention Schedule
- Part 3: Guidance for operation use

6. Implementation

6.1 Plan for implementation

The Information Governance Manager will ensure that this policy is available to all Divisional Managers within the Trust. It is then their responsibility to ensure that all staff groups within their area are directed to this policy.

Mandatory Data Security Awareness training covers the confidentiality of information and this is promoted within the trust on a regular basis.

6.2 Dissemination

This policy will be available on the Trust policy pages and a publication in the Trust Weekly Brief to inform staff of the update to the policy.

6.3 Training and awareness

All staff are mandated to complete Data Security Awareness training on an annual basis which covers all aspects of this policy.

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: <i>(Responsible for also ensuring actions are developed to address any areas of non-compliance)</i>	Frequency of reporting:
	WHAT?	HOW?	WHEN?	WHO?	WHERE?	WHEN?
4.2	All departmental managers are responsible for regular, localised monitoring of the quality of documentation and adherence to this policy.	Managers and senior clerical staff should annually undertake a survey of the records for which they are responsible to ensure that the standards, as detailed in this policy, are maintained.	Annually	Information Governance Officer/Manager	IGSG (monitored via the IG work plan)	Ad Hoc
4.2	Corporate Records Audit	Records Audit	Rolling programme	IG Team	Information Governance Steering Group	Following audit

8. Policy Review

This policy will be updated every three 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 [You should include external source documents and other Trust documents that are related to this Policy]

References:

Code:

NHS Code of Practice for Corporate Records Management	
The Data Protection Act 2018 (DPA18)	
EU General Data Protection Regulations 2016 (now UK GDPR and included within DPA18)	
Freedom of Information Act 2000	
The Human Rights Act 1998	
The Computer Misuse Act 1990	
Caldicott Principals	
NHS Data Security and Protection Toolkit	
Data Protection Good Practice – Information Commissioners Office	
NHS Employers – Policies and best practice procedures	
Benchmarking other NHS and Public Sector Data Protection practices	
Information Governance Policy	
Confidentiality Code of Conduct Policy	
Health Records Management Policy	
IT Security Policies	

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 chair(s) of the following committee's / groups for comments;

Committee
Information Governance Steering Group members

10.4 Approval Process

This policy will be approved at the Information Governance Steering Group

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:
2019	Minor update including, relevant dates and approval Appendices removed and available on the Information Governance Webpages	IGSG
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.	IGSG
23rd Dec 2020	Document extended for 3 months until March 2021 due to urgent COVID work	Deputy SIRO
31st March 2021	Document extended for 6 months as per Trust agreement 11.02.2021	Deputy SIRO
16th July 2021	Document review date amended as per the Key Documents policy 3 year approval update.	Deputy SIRO
12th April 2022	Document extended to the end of September to allow for thorough review	Deputy SIRO
Sept 2022	Re-write in line with national guidance update 2021	IGSG
22nd October 2025	Document extended for 6 months to allow time to ensure that all updates are included	Matthew Thurland
16th April 2026	Document extended for 6 months to allow time for review and update	Matthew Thurland

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;



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	Senior Information Risk Owner
----------------------------------	--------------------------------------

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	1 st September 2022		

Section 2

Activity being assessed (e.g. policy/procedure, document, service redesign, policy, strategy etc.)	Title: Corporate Records Management
What is the aim, purpose and/or intended outcomes of this Activity?	Policy document to inform all staff.

Trust Policy

Who will be affected by the development & implementation of this activity?	<input type="checkbox"/> Service User <input type="checkbox"/> Patient <input type="checkbox"/> Carers <input type="checkbox"/> Visitors	<input checked="" type="checkbox"/> Staff <input type="checkbox"/> Communities <input type="checkbox"/> Other _____
Is this:	<input checked="" type="checkbox"/> Review of an existing activity <input type="checkbox"/> New activity <input type="checkbox"/> 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.)	NHSX Code of Practice for Corporate Records Management 2021	
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		

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 <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
Age		X		
Disability		X		
Gender Reassignment		X		
Marriage & Civil Partnerships		X		
Pregnancy & Maternity		X		
Race including Traveling Communities		X		
Religion & Belief		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
Sex		X		
Sexual Orientation		X		
Other Vulnerable and Disadvantaged Groups (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling communities etc.)		X		
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		

Section 4

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
	None identified			
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)				

Section 5 - Please read and agree to the following Equality Statement

1. Equality Statement

Corporate Records Management Policy		
WAHT-CG-127	Page 19 of 21	Version 7.2

Trust Policy

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	Annie Osborne-Wylde
Date signed	1 st September 2022
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