Trust Policy	NHS Worcestershire Acute Hospitals NHS Trust

Pseudonymisation Policy

Department / Service:	Information
Originator:	Information Governance Manager
Accountable Director:	Director of Resources
Approved by:	Information Governance Steering Group Trust Management Committee
Date of Approval:	3rd July 2017
Review Date: **This is the most current document and should be used until a revised version is in place**	4th December 2020
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust
Target Departments	Departments handling and transferring patient information for: • Direct patient care • Non-direct patient care • Anonymised or Pseudonymised patient data for secondary care (SUS, CCG's etc.)
Target staff categories	Staff handling patient information for: • Direct patient care • Non-direct patient care • Anonymised or Pseudonymised patient data for secondary care (SUS, CCG's etc.)

Policy Overview:

This document seeks to provide all Trust staff that use patient information for direct/non-direct patient care or anonymised or pseudonymised patient data for secondary care purposes, with guidance to safeguard the confidentiality of personal confidential data (PCD).

Patient data used for none direct care (secondary) purposes must be **anonymised or Pseudonymised** in order to maintain personal confidentiality data in line with the Caldicott Principles and the Data Protect Act. In the light of the introduction of the general Data Protection Regulation (GDPR) in May 2018, this policy will be reviewed

Latest Amendments to this policy:

The policy only required minor updates including references to national policies or bodies – including:
Connection to health to NHS Digital, detail on Information standard update and adding references to national guidance

4th December 2020 – Document extended for 6 months whilst review process is undertaken
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

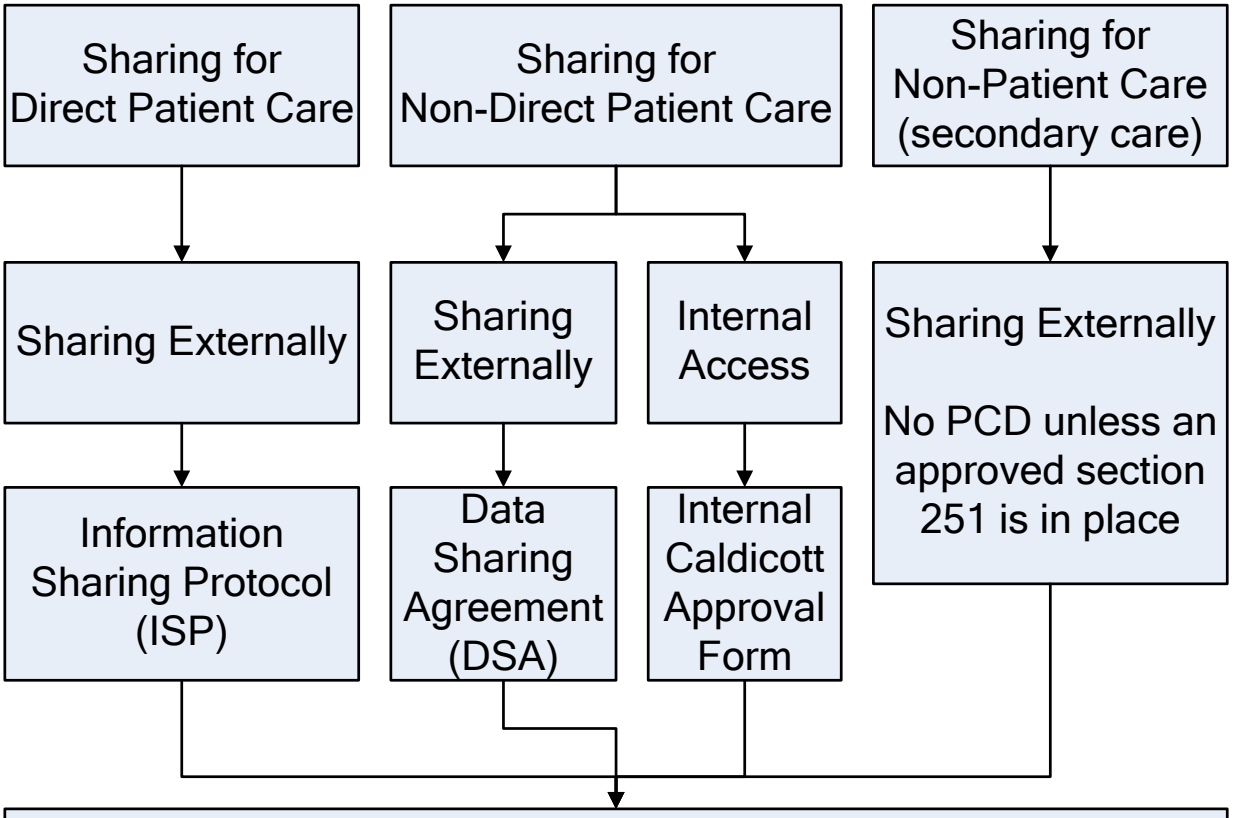
Supporting Documents

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

Quick Reference Guide

Sharing Information for Direct/Non-Direct Patient Care or Non-Patient/Secondary Care

This policy sets out the processes for sharing data capable of identifying an individual



All information sharing is logged on Data Sharing Register

All sharing agreements (Internal and External) are approved by the Caldicott Guardian/Information Governance Steering Group

All sharing agreements (Internal and External) are held in a register by the Information Governance Manager

1. Introduction

This Policy sets out the approach to be taken within the Worcestershire Acute Hospitals Trust (herein referred to as the Trust) to provide a documented process for all Trust staff who use data that may be capable of identifying an individual.

This Policy has been developed in line with guidance from:

- The Information Commissioner's Office "Anonymisation: managing data protection risk code of practice";
- The NHS Digital, Information Governance Toolkit Requirement 324 "The confidentiality of service user information is protected through use of pseudonymisation and anonymisation techniques where appropriate" delivered via the Trust's Pseudonymisation project.
- The Information Standards Board for Health and Social Care AMD 20/2010 "Anonymisation Standard for Publishing Health and Social Care Data";

The Data Protection Act 1998 (DPA) and the common law relating to confidentiality apply to all organisations. They require that the minimum personal data are used to satisfy any particular purpose. Organisations are required to respect people's private lives unless there is a lawful exemption to the Human Rights requirements and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned.

All NHS Commissioners and providers of NHS commissioned care must:

- Ensure appropriate changes are made to processes, systems and security mechanisms in order to facilitate the use of de-identified data in place of patient confidential data (PCD);
- Use the latest IG Toolkit to assist in implementation and assessment of compliance with policy and legal requirements;
- Ensure that relevant staff are aware of requirements and trained to use anonymised or pseudonymised data unless otherwise required by the demands of their role and approved as specified in this policy;
- Comply with the Information Standards AMD 20/2010 Anonymisation Standard for Publishing Health and Social Care Data.

Patient information or data may be shared following approval as set out below:

- Information Sharing Protocols (ISP) – Information shared for direct patient care
- Data Sharing Agreements (DSA) – Information shared for non-direct patient care with external organisations or processing for other organisations
- Internal Caldicott Authorisation to Access PCD for Non-Direct Purposes Form – Information accessed by Trust staff for non-direct patient care
- Data being shared for secondary care purposes which must be anonymised or Pseudonymised unless a current section 251 is in place.

2. Scope of this document

This policy applied to:

- All patient information processed for direct or non-direct patient care
- All data processing capable of identifying an individual, that may be involved in providing or publishing data for secondary use purposes e.g. anonymisation of patient data for the purpose of a service level evaluation; anonymisation of staff data for the purpose of monitoring sickness absence rates within the organisation.

NB All Patient data used for secondary purposes without a section 251 in place must be **anonymised or pseudonymised** in order to maintain patient confidentiality in line with the Caldicott Principles and the Data Protect Act.

3. Definitions

3.1 Patient/Personal Identifiable Data

This policy includes any one or more of the following patient data items wherever it/they may appear and irrespective of the name of any data field in which it/they may appear this commonly known within the NHS as Personal Confidential Data or PCD/PII: See Appendix 4 for PCD classification guidance.

- Name - including last name and any forename or aliases
- Address – including any current or past address of residence
- Date of birth
- Postcode - including any current or past postcode of residence
- NHS number
- Ethnic Category
- Local Patient identifier
- Hospital Spell number
- SUS spell ID
- Unique booking reference number
- Date of Death
- NI Number

This list is not exhaustive list

3.2 Patient Data categories

For the purposes of this policy, definitions of data categories are as follows and apply to data at individual record level:

Confidential patient identifiable data:

One or more of the data items specified in 3.1 can be viewed unmodified allowing:

- patients to be identified and differentiated within any subset of data;
- patient records to be linked across systems.

Pseudonymised:

One or more of the data items specified in 3.1 can be viewed modified allowing:

- Patients to be identified only via secure, Caldicott approved and managed access to related confidential patient identifiable data;
- Patients to be differentiated within any subset of data;
- Patients to be linked across systems.

Part anonymised:

One or more of the data items specified in 3.1 can be viewed modified:

- Allowing patients to be differentiated within any subset of data but not identified via other data sources and not allowing patients to be linked across systems or subsets of data.

Fully anonymised:

None of the data items specified in 3.1 can be viewed allowing:

- Differentiation by activity codes only – no patient differentiation or identification or linkage across systems or subsets of data.

3.3 Data Locations

This policy applies to data stored on hardware and equipment directly managed, owned or hired by each member organisation including but not limited to:

- Servers on Trust premises
- Servers on non- Trust premises
- Desktop computers on Trust premises
- Desktop computers on non- Trust premises
- Laptops, notebooks and netbooks
- PDAs, mobile phones
- Memory cards and memory sticks

3.4 Data Formats

This policy applies to data stored in the following formats including but not limited to:

- SQL Server (or equivalent) data repositories
- Microsoft Access (or equivalent) databases
- Microsoft Excel (or equivalent) spreadsheets
- Microsoft Word (or equivalent) documents
- Microsoft PowerPoint (or equivalent) presentations
- Microsoft Publisher (or equivalent)
- Plain text files in any format
- Zip files (or equivalent)
- Pdf files
- Emails and their attachments
- Graphics files in any format
- Other proprietary systems and their dedicated formats used to store or manipulate data.

3.5 Pseudonymisation

Pseudonymisation is the process of distinguishing identities. The aim of such a process (vs. anonymisation) is to be able to collect additional data relating to the same individual without having to know identity. Key-coded data is a classic example of pseudonymisation.

This applies to all electronic patient identifiable data, from large databases with thousands of records down to documents or files holding a single item of data, except those used for direct care and those information flows covered by Section 60/251 regulations for Public Health.

Driven through the Information Governance Toolkit, a national project, the Pseudonymisation Implementation Project (PIP), was set up to oversee and support local PIP work required to achieve this compliance. It will ensure that patient data is de-identified when used for secondary use purposes.

3.6 Anonymised Data

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity.

Anonymisation does not allow information about the same individual to be linked in the same way that Pseudonymisation does.

Anonymisation is more likely to be used for 'one-off' queries of data.

3.7 Secondary Use Service/Purposes

The Secondary Uses Service (SUS) is primarily a data warehouse that provides access to anonymous patient-based data for purposes other than direct clinical care such as:

- healthcare planning
- commissioning services
- public health
- national policy development

SUS is delivered by the Health and Social Care Information Centre (HSCIC) where Patient Identifiable Data is used for work not directly related to the care of the patient/service user.

Examples of secondary uses are commissioning, payment by results (PbR), performance management, capacity planning, service redesign and benchmarking.

3.8 Primary Use/Healthcare Purposes

Primary use of patient data covers two types, those that directly contribute to the diagnosis, care and treatment of an individual and those used in the audit/assurance of the quality of healthcare provider.

4. Responsibility and Duties

4.1 Chief Executive

The Chief Executive has overall responsibility for the Trust's Information Governance programme and ensuring that this operates effectively. Operational responsibility for Information Governance lies with the Director of Resources, as the Senior Risk Owner (SIRO).

4.2 Caldicott Guardian

The Chief Medical Director (Caldicott Guardian) is responsible to the Board of Directors and Chief Executive in relation to Information Governance.

The Caldicott Guardian must:

- Review and authorise staff access to PCD for Non-Direct Care Purposes;
- Inform the Information Governance Manager of staff approvals of access to PCD following completion of the 'Internal Caldicott Authorisation to Access PCD for Non-Direct Care Purposes Form' (Appendix 5) should be forwarded and filed by the Information Governance Team.

4.3 Operational Managers/Senior Staff

Managers and senior staff have particular responsibility for ensuring that Information Governance practices and procedures are maintained in accordance with the policy.

Operational Managers/Senior Staff must:

- Identify staff that have a justified purpose to access PCD for non-direct or secondary use purposes.
- Ensure that their staff are appropriately trained, utilising the Information Governance Training Tool;
- Regularly review the appropriateness of staff access to PCD;
- Organise the removal of staff access rights to PCD, where there is no longer a need for staff to access PCD for non-direct or secondary use purposes;
- Inform the Information Governance Manager of staff that no longer require access to PCD;
- Inform the Caldicott Guardian of new staff that requires access to PCD for Non-Direct/Secondary Use purposes by completing the 'Internal Caldicott Authorisation to Access PCD for Non-Direct Purposes Form' in Appendix 5 sending it to the Caldicott Guardian for approval.

4.4 Information Governance Manager

The Information Governance Manager must:

- Maintain a register of staff who have access to PCD for Non-Direct or Secondary Use purposes, including:
- Information Sharing Protocols (ISP) – Information shared for direct patient care
- Data Sharing Agreements (DSA) – Information shared for non-direct patient care with external organisations or processing for other organisations
- Internal Caldicott Authorisation to Access PCD for Non-Direct Care Purposes Form – Information accessed by Trust staff for non-direct patient care
- Inform the Information Governance Steering Group (IGSG) of any new agreements.

4.5 All Staff

All Staff are responsible for ensuring that good Information Governance is at the heart of the work they do when handling personal or sensitive information.

Staff with access to PCD must:

- Keep PCD confidential;
- Only use/transfer PCD when authorised to do so;
- Transfer PCD in a secure manner as per agreed Safe Haven procedures;
- When transferring PCD via e-mail to another NHS organisation, NHSmail should be used by both sender and recipients. See the E-mail Usage Policy for further details;
- All other transfers of PCD should be via approved secure methods and/or secure networks;
- Anonymise PCD where possible. In any case, the minimum amount of PCD necessary should be used. See the Caldicott Principles in Appendix 1 for further details.

4.6 Specific to Publication

- Ensure that the publication of Health and Social Care Data is compliant with the Information Standards Board standard ISB 1523, Anonymisation Standard for Publishing Health and Social Care Data.
- Ensure that publication of any data derived from data sets capable of identifying an individual is anonymised in accordance with the Information Commissioner's Anonymisation Code of Practice.
- The Caldicott Form must be completed and signed-off by:
    - The Information Governance Steering Group for publication of anonymised non-patient data sets
    - The Information Governance Steering Group and Caldicott Guardian for the publication of anonymised patient data sets.

5. Principles of Policy

5.1 Patient Identifiable Data should generally only be used where:

- There is a direct care-related need to use such data. Patient level data should not contain identifiers when they are used for purposes other than the direct care of patients;
- Patient consent has been received;
- Section 60/251 regulations apply for Public Health data; When using PCD for Secondary Use purposes, data must be anonymised/de-identified as much is practically possible;
- Data itself cannot be labelled as primary or secondary use data; it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them;

5.2 Principles for Secure Handling

- Safe Haven procedures must be used at all times when handling and sharing PCD, regardless of whether the data is being used for healthcare purposes or secondary use purposes;
- Staff who have access to PCD for Non-Direct care or Secondary Use purposes should be identified;
- Access to PCD for Secondary Use purposes should be appropriately authorised by the Trust's Caldicott Guardian;
- Access to PCD should be restricted to authorised users only;
- A register of staff with access to PCD for Non-Direct care or Secondary Use purposes should be created and maintained;
- Staff access to PCD for Non-Direct care or Secondary Use purposes should be periodically reviewed, to ensure that the level of access to PCD is still relevant and appropriate.

5.3 Sharing information for the purpose of direct patient care

The Trust has a high level (Tier 2) Information Sharing Protocol (ISP) in place which all health and social care organisations in Worcestershire have signed up to and which provides the general framework and principles for sharing data for direct patient care purposes. (See Appendix 2 for list of organisations and Appendix 7 for the Trusts Tier 3 ISP Template)

Where data is required to be shared for patient care and it is of a personal or sensitive nature or the data items are above and beyond the information we routinely share or with an organisation or organisations who the Trust would not routinely share information with, then a Tier 3 ISP should be developed and approved. The Tier 2 and Tier 3 ISPs along with any Data Sharing Agreements (DSA's) are logged on the Data Sharing Register. If information is requested to be shared for the purpose of direct patient care which is outside of the routine information shared to support patient care or is of a sensitive nature, contact the Information

Governance Manager who will liaise with the organisation and develop and gain approval for a Tier 3 ISP. When completed and approved this will be added to the Data Sharing Register and signed off by the Caldicott Guardian.

5.4 Sharing information for the purpose of non-direct patient care or processing for other organisations

If the information requested is for non-direct care purposes or processing data on behalf of another organisation or vice versa - a Data Sharing Agreement is required. Contact the Head of Information and follow the process outlined below; See Appendix 6 for the Trusts DSA Template and Appendix 3 for the process for DSA authorisation

5.5 Data Sharing Register

A Data Sharing Register is in place which covers any ad hoc or regular information or data sharing requests with any external organisations over and above what is available via SUS. Unless it's a contractual requirement (e.g. SUS/ CQUINs), information, contracting or operational staff must not release information unless authorised and included on the register. All returns will be Quality Assured for data quality purposes by the Head of Information and will require sign off by either the Director of Finance or the Chief Operating Officer along with the Caldicott Guardian.

The Register will include all:

- Information Sharing Protocols (ISP) – Information shared for direct patient care
- Data Sharing Agreements (DSA) – Information shared for non-direct patient care with external organisations or processing for other organisations
- Internal Caldicott Authorisation to Access PCD for Non-Direct Purposes Form – Information accessed by Trust staff for non-direct patient care
- Anonymised or pseudonymised for secondary care purposes, including any section 251 agreements

A register which contains all Information Sharing Agreements (Tier 2 and Tier 3's) along with all DSA's will be maintained by the Information Governance Manager and can be found via the following link: (To be added with possibility of storing it on internal website for greater access to other departments)

5.6 Pseudonymisation Controls

In addition to the member organisation's Safe Haven procedures, policies and staff training, the member organisation's currently employs the following Pseudonymisation Controls:

- When data warehouse suppliers and systems are refreshed, Pseudonymisation controls and technology should be implemented where possible, including relevant logging and auditing facilities;
- When releasing patient level data to other staff or third parties (for example consultancies employed by the member organisation's) where no data sharing arrangement is in place, information staff will deploy a Pseudonymisation algorithm to all patient identifiable data items. This will ensure there is linkage between records without compromising patient confidentiality. Pseudonymisation keys will not be released to staff outside of the Information Team and will be changed on a regular basis.

5.7 Publishing Health and Social Care Data

The Trust is mandated to comply with ISB 1523. This requires individuals prior to publishing, to confirm with the organisation's Caldicott Guardian and other key stakeholders, mainly the

members of the Information Governance Steering Group, that the information to be published does not identify individuals, and this confirmation MUST be recorded and be available subsequently on request in the Caldicott form.

Please refer to specific responsibilities outlined in section 4.5

This anonymisation standard for publishing health and social care data is required in order to address the difficult issues involved in anonymising complex data sets. This process standard provides an agreed and standardised approach, grounded in the law, enabling organisations to:

- Distinguish between identifying and non-identifying information, and
- Deploy a standard approach and a set of standard tools to anonymise information to ensure that, as far as it is reasonably practicable to do so, information published does not identify individuals.

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 Information Governance training covers the secure transferral of information and this is promoted within the Trust on a regular basis.

6.2 Dissemination

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

6.3 Training and awareness

All staff must complete IG training on an annual basis and familiarise themselves with the content of key policies.

Staff who need to anonymise data must be familiar with the use the tool. (OpenPseudononymiser)

7. Monitoring and compliance

See table on next page

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 9 Point 5.3	Data Sharing Register	Review outputs against those listed on the register	When information Requests are received	Dept Manager/Information Manager	Information Governance Steering Group	Reported via bi-monthly meetings when required

8. Policy Review

This policy will be reviewed and 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. The Key Documents Approval Group will ratify and publish the policy.

9. References

References:	Code:
The ICO Guidance: Anonymisation: managing data protection risk code of practice	
NHS Digital, Information Governance Toolkit Requirement 324	
The ISB AMD 20/2010 Anonymisation Standard for Publishing Health and Social Care Data	
Code of Conduct in Respect of Confidentiality	
Safe Haven Policy	
Incident Reporting Policy	
Information Governance Policy	
Information Security Policy	
Internet and Email Policy	

10. Background

10.1 Equality requirements

None - See supporting Document 1

10.2 Financial risk assessment

None - See Supporting Document 2

10.3 Consultation

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

Contribution List

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

Designation
Director of Finance (Chair)
Assistant Director of Information and Performance
Director of IT and Asset Management
Company Secretary
Information Governance Manager
Information Governance Officer
Human Resources representative
IT Services representative
Head of Legal Services
Caldicott Guardian

Director of Nursing representative

This key document has been circulated to the chair(s) of the following committee's / groups for comments;

Committee
Information Governance Steering Group
Key Documents Approval Group

10.4 Approval Process

This policy will be agreed at the Information Governance Steering Group and ratified by the Key Documents Approval 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:
Nov 2014	Policy Created	IG Manager
June 2017	The policy only required minor updates including references to national policies or bodies – including: Connection to health to NHS Digital, detail on Information standard update and adding references to national guidance	IG Manager

Caldicott Principles Appendix 1

Worcestershire Acute Hospitals NHS Trust

Caldicott Principles

What is Caldicott?
The term Caldicott refers to a review commissioned by the Chief Medical Officer. A review committee, under the chairmanship of Dame Fiona Caldicott, investigated ways in which patient information is used in the NHS. The review committee also made a number of recommendations aimed at improving the way the NHS handles and protects patient information.

What is a Caldicott Guardian?
A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information-sharing.

The Guardian plays a key role in ensuring that the Trust satisfies the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to facilitate and enable information sharing and advise on options for lawful and ethical processing of information as required.

The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board level.

These recommendations are summarised by the Six Caldicott Principles:

1	**Justify the purpose**
2	**Do not use patient-identifiable information unless it is absolutely necessary**
3	**Use the minimum necessary patient-identifiable information**
4	**Access to patient-identifiable information should be on a strict need to know basis**
5	**Everyone should be aware of their responsibilities**
6	**Understand and comply with the Law**
7	**The duty to share information can be as important as the duty to protect patient confidentiality**

Tier 2 Sharing Partners Appendix 2

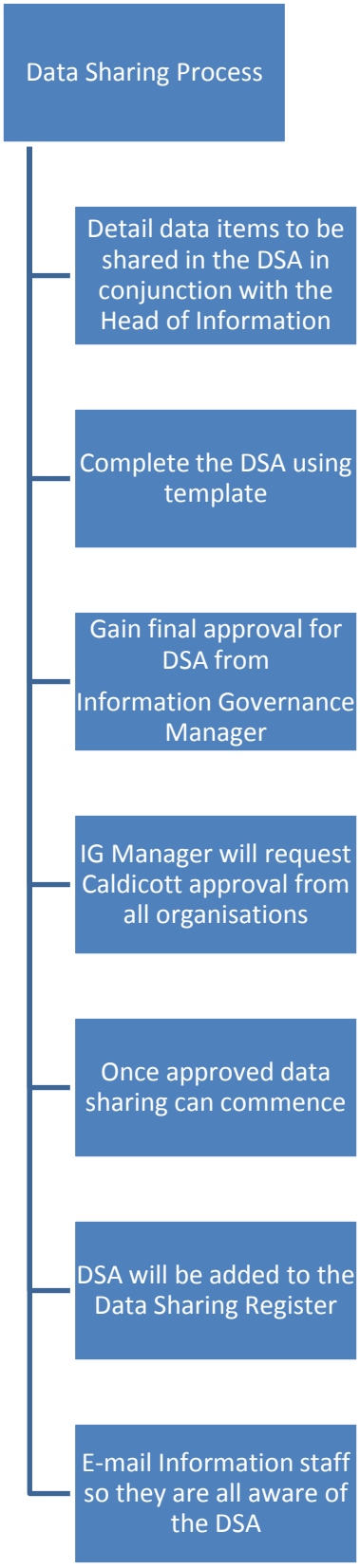
Worcestershire Acute Hospitals NHS Trust

Adults Tier 2 - General Protocol for Information Sharing Across Worcestershire

Worcestershire Acute Hospitals NHS Trust
Worcestershire Health and Care NHS Trust
Worcestershire County Council
NHS South Worcestershire Clinical Commissioning Group
NHS Redditch and Bromsgrove Clinical Commissioning Group
NHS Wyre Forest Clinical Commissioning Group
Arden Commissioning Support Service
NHS England – Arden, Hereford and Worcestershire Local Area Team
West Midlands Ambulance Service NHS Trust
Care UK – GP out of hour's services
NHS 111
St. Richard's Hospice
Kemp Hospice
Primrose Hospice
Worcestershire General Practices

Childrens Tier 2 -Protocol for sharing information between the Childrens Trust Agencies working for children and young people in Worcestershire:

Public Health England
Arden Commissioning Support
West Midlands Ambulance Service
NHS England
Worcestershire Health & Care Trust
CCG's
Worcestershire County Council
Wychavon District Council
Wyre Forest District Council
Bromsgrove District Council
Malvern Hills District Council
Worcestershire Council for Voluntary Youth Services
West Mercia Police
Harmoni (111)
WAG


Data Sharing Process
Detail data items to be shared in the DSA in conjunction with the Head of Information
Complete the DSA using template
Gain final approval for DSA from Information Governance Manager
IG Manager will request Caldicott approval from all organisations
Once approved data sharing can commence
DSA will be added to the Data Sharing Register
E-mail Information staff so they are all aware of the DSA

Appendix 4
PID/PCD Definitions

Worcestershire NHS
Acute Hospitals NHS Trust

Person Identifiable Data (PID) / Personal Confidential Data (PCD)

PCD is a term used in the Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept private or secret and includes dead as well as living people.

The review interpreted 'personal' as including the Data Protection Act definition of personal data, but included data relating to the deceased as well as living people, and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.

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, however other information, when combined, could potentially identify an individual. It can relate to any individual - this includes members of staff, patients or members of the public.

Personal Data		**Sensitive Data**
A non-sensitive identifier, the disclosure of which, is unlikely to cause damage or distress to an individual or third party		Information , the disclosure of which, is likely to cause damage or distress to an individual or third party
Defined in the Data Protection Act as: Data relating to a living individual who can be identified from those data (e.g. an employees name) or identified from those data and other information which is in the possession of the data controller (e.g. an employees payroll number)		**Defined in the Data Protection Act as:** • Personal data falling within a certain criteria (specified below) • information that may lead to damage or distress (e.g. breach of privacy, financial loss etc)
All personal or sensitive information should be processed/transferred in line with the Caldicott Principles		
Personal Information includes: • Name • Address (home or business) • Postcode • NHS Number • NI Number • Local identifier (Hospital Number etc) • Date of Birth • Date of Death or Diagnosis etc • Email Address • Telephone number • Payroll number • Occupation • Sex • Ethnic Group • Driving Licence number		**Sensitive information includes:** • Racial/Ethnic Origin • Political Opinions • Religious Beliefs • Trade Union Membership • Physical or Mental Health or Condition • Sexual Life • Alleged and Commissioned Criminal Offences And may include: • Bank, Financial or Credit Card Details • Mothers Maiden Name • Tax, Benefit or Pension Records
For NHS common law duty of confidence purposes, individual identifiers/Personal Identifiable Data also applies to deceased patients		This type of data must be protected by the strongest security measures practicable.
Other examples of personal information may include: • Pictures, Photographs, videos • Audio tapes or Other images of patients • Rare Diseases • Drug treatments		
Confidential Material Confidential material is any information, in any form, that is generally disclosed from one person to another (e.g. Patient to Clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It must be treated as such so long as it remains capable of identifying the individual it relates to. All personal data relating to the NHS should always be classified as **NHS CONFIDENTIAL**		
Business Information Business information, while not relating to a specific individual, should also be treated as **confidential** if not in the public domain. If this kind of information is lost or misplaced, or its integrity is affected, it could impact adversely on individuals, the organisation and/or the wider community. Information on financial arrangements specific to an organisation's business operations, finance or security is also likely to be deemed 'confidential' or 'sensitive'.		

Appendix 5 Internal Caldicott Form	Worcestershire NHS Acute Hospitals NHS Trust

Appendix 5 – Internal Caldicott Authorisation to Access PCD for Non-Direct Care Purposes

This Form is to be completed by the relevant Service Manager when it is necessary for a member of staff to access Patient Confidential Data (PCD) for Secondary Use Purposes. This form should be sent to the Caldicott Guardian for authorisation and risk assessment.

Name			
Contact Number		Department	
Email Address		Directorate	
Details of Data to be Accessed for Non-Direct Care Purposes			
Data Description			
Types of Data User will be accessing: (Circle)	Name	DoB	Gender
	Ethnicity	Medical Details	Address/Postcode
	Other (please specify)		
Reason of Accessing PCD			
Format of Data Transfer (i.e. electronic/paper based):			
Frequency of Data Access (i.e. One-Off, Monthly, Quarterly, Annually, etc.):			
Proposed mechanisms to secure the data being accessed:			
If applicable, what systems are used to access the PCD for Non-Direct Care Purposes:			
LINE MANAGERS DETAILS			
Name		Email Address	
Contact Number		Department	
Date		Directorate	
Signature			
CALDICOTT GUARDIAN USE ONLY			
Name (PRINT)			
Position			
Signature			
Date			

Appendix 6
Data Sharing Agreement

Worcestershire Acute Hospitals NHS Trust

Reference:	
Contract Reference	N/A

Parties to the Agreement

This Data Sharing Agreement (Agreement) is drawn up between:

Add name and address here

And: (**Data Recipient)**

Organisation Name:	Worcestershire Acute Hospital NHS Trust
Organisation Address:	Charles Hasting Way Worcester WR5 1DD

And: (**if applicable, Data Processor**)

Organisation Name:	Worcestershire Acute Hospital NHS Trust
Organisation Address:	Charles Hasting Way Worcester WR5 1DD

Scope of Agreement

Start Date		End Date	

Appendix 6 Data Sharing Agreement	Worcestershire Acute Hospitals NHS Trust

Data Details

☐ Anonymised

☐ Patient Level, pseudonymised	
☐ Sensitive Data	
☐ ONS Data	
Purpose	

☐ Weakly pseudonymised Identifier	
Purpose	

☐ Patient Level, identifiable	
Legal Gateway	Contract been agreed & signed
Purpose	Worcester Royal Hospital to submitted the data to SUS on behalf of the sender:

Specific Conditions

The Data Sharing Contract referenced at the beginning of this agreement provides the high level assurances around the transfer and governance of data supplied to the data recipient. In addition to those assurances sought in the Contract the following conditions also apply:

Use of the data provided under this agreement is for the sole purpose set out above.

Staff processing the data must be suitably trained and made aware of their responsibilities in handling the Data.

The Data must not be shared with any other organisation or named individual not explicitly referred to within this agreement.

If the information received from the supplier is subject to a request under the Freedom of Information Act, then the supplier must be consulted before a response is provided.

The Data must not be shared with any third party in the format in which it is provided to you by the supplier.

Use of the Data complies with any specific legislation in relation to the Data provided by the supplier.

Information tools derived from this Data will not be provided to other organisations without the specific consent of the supplier

The supplier retains copyright of this information, unless otherwise instructed and this must be cited correctly.

.

Any publications derived from this Data by any party must be subject to the following guidance:

ONS Guidance for Health Statistics: http://www.ons.gov.uk/ons/guide-method/best-practice/disclosure-control-of-health-statistics/index.html

ONS policy on protecting confidentiality within birth and death statistics and the Code of Practice for Official Statistics: http://www.ons.gov.uk/ons/guide-method/best-practice/disclosure-control-policy-for-birth-and-death-statistics/index.html

Anonymisation Standard for Publishing Health and Social Care Data: http://www.isb.nhs.uk/library/standard/128

Before undertaking any publication activity using this Data or any derived information, the Data Recipient will undertake an organisational Risk Assessment Exercise to ensure compliance with the above guidelines.

The supplier reserves the right to undertake an audit with respect to the use and storage of the Data to ensure that the terms of this agreement are being abided by.

Data Access

Under the terms of this agreement, access to the Data must be managed, auditable and restricted to those individuals who need to process the Data for the specific purpose/s outlined above.

Annex A: Data Security Requirements

As a Data Controller / Data Custodian and, (if applicable), Data Processor, with respect to the data being provided by the supplier, the Data Recipient undertakes to ensure that:

It implements and maintains security standards, processes, procedures, practice and controls appropriate to the nature of the Data received and the harm that would be caused by its loss or disclosure

It processes personal or sensitive personal data only for health and social care purposes, and only for purposes described in this data sharing agreement which it assures are also consistent with the purposes recorded in the Data Recipient's data protection registration with the Information Commissioner's Office

It processes the minimum data necessary (e.g. using age range rather than age if sufficient)

Access to the Data is limited to those employees who need access to the Data for the purpose stated in the Agreement

It ensures that the Data supplied is stored on a secure system password protected and that all computer terminals and other means of access are maintained securely in secure premises

It ensures the rights of individuals are met, such as satisfying subject access requests received, ensuring data accuracy and correcting errors, and handling objections and complaints

It destroys the Data once it is no longer required for the purpose for which it was collected and confirming destruction to the supplier

It ensures all employees with access to the Data understand the confidential nature of the Data and their responsibilities

It reports immediately to the supplier any security incidents relating to use of the supplied Data, and any instances of breach of any of the terms of this Agreement

It adheres to the security requirements set out in the overarching Data Sharing Contract.

Annex B: Specific Terms and Conditions

Specific Terms and Conditions
Data containing identifiers supplied must be stored in a controlled environment.

Annex C: Data Transfer Method

The Data will be sent using an appropriate secure electronic file transfer (SEFT) mechanism to a Permitted User:

☐ Data Depot (Non-Identifiable data < 2Gb)

The user will receive a request to register via email. Once registered the user will receive an email informing them that a file is ready to be downloaded. The user will log in to the portal using their user name and password (SSO account). The data will be transmitted using a 128 AES encryption mechanism.

☐ Tibco MFT (Non-Identifiable Data or Identifiable Data, no size limit)

The user will receive their user name and password via email and/or telephone. The user will log in to the portal using their user name and password. The data will be transmitted using a 256 AES encryption mechanism.

☐ Tibco Slingshot (Non-Identifiable Data or Identifiable Data, no size limit)

The user will receive an email informing them that a file has been sent to them. The user will access a link in the email and register their details. Once authenticated they may download the file. The data will be transmitted using a 256 AES encryption mechanism.

☐ HSCIC approved RPC transfer method (Non-Identifiable Data or Identifiable Data)

Description:
Dedicated, secure private networks are in place. Data will be transferred securely via sFTP, SFT, NHSmail and/or SQL data push from the RPC (as detailed within RPC SLSP document)

☐ Controlled access to SUS, PARs and Choose and Book

The named person must not share their password with any other person at any time. Once the data has landed at the organisation, the security of the data is not the responsibility of the supplier

Agreement Signatures

for and on behalf of: *<insert data recipient name>*	
Organisation Name:	
Organisation Address:	
Signature:	
Name:	
Role:	
Date:	1

for and on behalf of: Worcestershire Acute Hospital NHS Trust	
Organisation Name:	Worcestershire Acute Hospital NHS Trust
Organisation Address:	Charles Hasting Way Worcester WR5 1DD
Signature:	
Name:	
Role:	Caldicott Guardian
Date:	dd/mm/yyy

Appendix 7 ISP Tier 3 Template	Worcestershire Acute Hospitals NHS Trust

Please ensure all items in Red are updated

[Name of Service]

Information Sharing Protocol

Version:	
Ratified by (name of Committee):	Information Governance Steering Group
Date ratified:	
Date issued:	
Expiry date: (Document is not valid after this date)	
Review date:	
Lead Executive/Director:	Mark Wake
Name of originator/author:	Annie Osborne-Wylde
Target audience:	Service Users

Appendix 7
ISP Tier 3 Template

Worcestershire Acute Hospitals NHS Trust

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
Add names of leads etc from sharing departments	Job title
Add names of leads etc from sharing departments	Job title
Add names of leads etc from sharing departments or delete	Job title
Add names of leads etc from sharing departments or delete	Job title

Circulated to the following individuals for consultation

Name	Designation
Mark Wake	Caldicott Guardian
Information Governance Steering Group	Members of the Acute Information Governance Steering Group

Appendix 7 ISP Tier 3 Template	Worcestershire Acute Hospitals NHS Trust

Contents

Appendix 7 ISP Tier 3 Template	Worcestershire Acute Hospitals NHS Trust

Introduction

Information Sharing Protocol to [enter broad purpose here]

Partner agencies covered by this protocol

Agency (Division / Section / team)	Protocol Lead person (Name & job title)	Protocol signatory (Name & job title)
Worcestershire Acute Hospitals NHS Trust – add department	Department lead	Name and Job Title
Add name of sharing partner	Department lead	Name and Job Title
Add name of sharing partner or delete box	Department lead	Name and Job Title

Purposes of sharing information covered by this protocol

- Add why information is shared/the purpose of the sharing
- Add why information is shared/the purpose of the sharing
- Add why information is shared/the purpose of the sharing
- Add why information is shared/the purpose of the sharing

The information covered by this protocol can only be used for the purpose for which it was collected. If any of the Partners to the protocol want to change the purpose, all Partners need to agree to the change. If a Partner to the protocol wants any of the data for further statistical purposes, personal information should be anonymised.

This protocol has been developed bearing in mind the Data Protection Act 1998, the Human Rights Act 1998 and the Freedom of Information Act 2000.

Relationship of this Protocol to other Protocols:

This Protocol sits at Tier three in a framework for Worcestershire. Its relationship to other protocols can be seen in the table below:

Tier One	Worcestershire Standard for Sharing Personal Data
Tier Two	General Protocol for Sharing Information across Health and Social Care in Worcestershire (delete as appropriate) Worcs Adult General Information Sharing Protocol Worcs Children and Young People Information Sharing Protocol

Appendix 6 ISP Template	Worcestershire Acute Hospitals NHS Trust

Tier Three	Enter name of this Protocol here

Specific information which will be shared

Data Categories – add or delete as appropriate	May include….
Demographics	Please list: for example, name, DoB, Address/Postcode, NHS number, GP
Clinical Details	Please list: for example if basic or full details, clinical history, test results or specify specialty information to be shared
Specific department info	Please list: for example a certain type of information that may be in referral forms or clinical data forms

What is the legal basis for this sharing?

Acts – Delete or add as appropriate	Further details if needed
Data Protection Act 1998	
Human Rights Act 1998	
The Health and Social Care Act 2012	
The Common Law Duty of Confidentiality	
The Caldicott Principles 2	
Mental Capacity Act 2005	
Equality Act 2010	

All information shared for the purpose of this protocol should be accurate, current and should not be shared indefinitely. The quantity and coverage of data shared should be directly related to the purpose of sharing, and not excessive.

Appendix 7 ISP Tier 3 Template	Worcestershire NHS Acute Hospitals NHS Trust

Processes for sharing the information

Data Category	Partner collecting this information	Partner receiving the information	DP Condition for sharing	Caveats on the sharing	Retention periods
Example: Basic Demographic as detailed in section 5	Data form completed and faxed	Data form received	Explicit consent or legal basis	None as for patient care	As per NHS corporate Records Retention Schedule
Example: Basic Demographic as detailed in section 5	Held in electronic clinical system	Access via electronic clinical system	For direct patient care	None as for patient care	As per NHS corporate Records Retention Schedule

OR

Delete as appropriate - Insert a flow diagram showing process for sharing

Processes for informing individuals about use of their data

Delete as appropriate:

The sharing organisation is a partner in the Tier 2 Worcestershire General Information Sharing Protocol and consent to use data is included in this protocol.

There is no Tier 2 Information Sharing Protocol between the organisation and individuals must to made aware of the sharing of their information.

This Protocol will be a public document and will be included in the Publication Schemes of the partners under the Freedom of Information Act.

Processes for dealing with Subject Access Requests and Complaints

Delete as appropriate:

The sharing organisation is a partner in the Tier 2 Worcestershire General Information Sharing Protocol and Subject Access Requests and Complaints procedures are included.

There is no Tier 2 Information Sharing Protocol between the organisation and partners must ensure that they any Subject Access Requests and Complaints are dealt with in occordace to the partner organisations policys.

Processes for informing and guiding staff about the arrangements

Delete as appropriate:

The sharing organisation is a partner in the Tier 2 Worcestershire General Information Sharing Protocol and process for informing staff are included.

There is no Tier 2 Information Sharing Protocol between the organisation and partners must ensure that they are providing guidance to their staff for processing the shared information.

Additional requirements, including security

Delete as appropriate:

The sharing organisation is a partner in the Tier 2 Worcestershire General Information Sharing Protocol and additional requirements are included.

There is no Tier 2 Information Sharing Protocol between the organisation and partners must ensure that they provide information around security of shared data.

Implementation Plan

Please create and insert a local implementation plan as an appendix 2

Or Partner Responsibility

Each Partner must ensure that this protocol is made available to all staff.

All staff must ensure that they have read and are familiar with the contents of this protocol.

Each Partner will undertake to provide its staff with appropriate training and information to ensure their compliance with this protocol, the laws of confidentiality, Human Rights Act 1998, Data Protection Act 1998 and the Mental Capacity Act 2005. All staff shall be made aware that disclosure of information (whether inadvertently or intentionally) which cannot be justified under this protocol, could make them liable to disciplinary action.

Partner sign off

This Protocol applies from…….. [enter date] and shall be reviewed annually thereafter. The Review shall be undertaken by a representative from each Partner and Data Protection Officers/Caldicott Guardians as appropriate.

Partners to this Protocol are:

Agency	Name and job title	Signature
Worcestershire Acute Hospitals NHS Trust	Name and Job Tile	
Add sharing partner organisation	Name and Job Tile	
Add sharing partner organisation or delete	Name and Job Tile	
Add sharing partner organisation or delete	Name and Job Tile	

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:**	N	
	• Race		
	• Ethnic origins (including gypsies and travellers)		
	• Nationality		
	• Gender		
	• Culture		
	• Religion or belief		
	• Sexual orientation including lesbian, gay and bisexual people		
	• Age		
2.	**Is there any evidence that some groups are affected differently?**	N	
3.	**If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?**	N	
4.	**Is the impact of the Policy/guidance likely to be negative?**	N	
5.	**If so can the impact be avoided?**		
6.	**What alternatives are there to achieving the Policy/guidance without the impact?**		
7.	**Can we reduce the impact by taking different action?**		

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	N
2.	Does the implementation of this document require additional revenue	N
3.	Does the implementation of this document require additional manpower	N
4.	Does the implementation of this document release any manpower costs through a change in practice	N
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	N
	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