Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Information Management Systems (Registration) Policy

This procedural document supersedes: CORP/ICT 3 v.6 – Information Management Systems (Registration) Policy.

Did you print this document yourself?
The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours**

Executive Sponsor(s):	Dan Howard – Chief Information Officer (CIO) & Senior Information Risk Owner (SIRO)
Name and title of author/reviewer: (this version)	Roy G Underwood, Head of Information Governance / Data Protection Officer
Date revised:	January 2024
Approved by (Committee/Group):	Information Governance Group
Date of approval:	22 January 2024
Date issued:	28 February 2024
Next review date:	January 2027
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
7	January 2024	• Tri-Annual Review • Amendments to reflect on the UK GDPR & the DPA 2018 • The completion of the NHSE DTAC (Digital Technology Assessment Criteria), which also includes a section on Clinical Safety with references to DCB0129 and DCB0160 • Reference to guidance from the Information Governance, Caldicott & SIRO Support (IGC&SS) Team • Removal *in toto* of the draft DPIA Mask at Appendix 4, where the latest 'in-use' version is now available directly from the Policy Page	Roy Underwood Rhona McCleery Jerome Boniface
6	July 2020	• Amendment to Appendix 1, Information Management System (IMS) Registration Proforma and Appendix 4, the Data Protection Impact Assessment (DPIA)	Roy Underwood
5	Sept 2018	• Tri-Annual review • Policy reviews to include references to the EUs General Data Protection Regulation (GDPR) and the UKs Data Protection Act 2018 • Include Data Privacy Impact Assessment (DPIA) • Amend the Records Management Code of Practice reference • Amend the 'Policy at a Glance' table • Change-over from the IG Toolkit to the Data Security and Protection (DSP) Toolkit for reporting to the Trust Information Governance Group	Roy Underwood
4	April 2015	• Tri-Annual review • Policy Reformat • Include IG/RA Checklist • Amendments to Monitoring arrangements	Roy Underwood Martin Boyda
3	Decem ber 2011	• Format updated • Complete rewrite, especially concerning the Trust SIRO and the associated IAOs and IAAs • Clinical Safety Officer (CSO) iaw DSCNs 14 & 18/2009	Roy Underwood Mark Norwood
2	January 2007	Bi-annual review, incorporating amendments for: - Supersedes the original 'Database Management Policy v1' - The inclusion of the main Trust Patient Clinical Systems – page 4 - An access control policy statement – page 4	Roy Underwood Dr Emyr W Jones
1	June 2004	Annual Review – no change	Roy Underwood Dr Emyr W Jones

Contents

Page No.

1. INTRODUCTION

Failure to store and process personal data in accordance with the Data Protection Act 2018 and the GDPR could lead to your prosecution in a court of law.

In order to ensure that the Trust, and its employees, comply with the UKs General Data Protection Regulation (GDPR), the Data Protection Act 2018, and NHS Digital's guidance "Records Management for Health and Social Care 2021", the following policy must be followed for any personal data that you are currently holding, or are considering holding, on a computerised system or otherwise.

Software applications used to store electronic data may be termed as "Database Software", "Spreadsheet Software" or "Word Processing Software". However, any set of structured data stored on any system will constitute a "Trust Information Asset", including the Trust's main Patient Records systems, and any other personal and/or non-personal but significant records management Systems.

If you're not sure, ask the Information Governance, Caldicott & SIRO Support (IGC&SS) Team: dbth.dpo@nhs.net

1.1 Policy at a Glance (Included in Appendix 3 and 4 for Applicants use)

Information Asset Registration Matrix	New Trust Core System Yes, No or N/A	In-House Division or Departmental System/Database Yes, No or N/A	3rd Party, Divisional, or Departmental System/Database Yes, No or N/A
Project Agreed – including Funding and Staffing arrangements - at an appropriate and authorised Trust Level			
Information Asset Owner (IAO) and Administrator (IAA) identified and appointed; some additional IG/RA training may be required at this point			
IG and RA Risks identified and mitigated (<5) by Head of IG and system IAO/IAA (Appendix 3 Completed)			
Is a Data Privacy Impact Assessment (DPIA) required as at Appendix 4?			
Is a Privacy Notice (PN) required?			
Is a Digital Technology Assessment Criteria (DTAC) required where advice and assistance can be sought from the IGC&SS Team			
Is Clinical Safety Reporting advice required from the Trust Chief Nursing Information Officer			
Project Registered with Head of Information			

Governance | Trust DPO			
IG Committee sign-off (where necessary)			

2. PURPOSE

This policy sets out to ensure best practice in the storing and processing of personal data. The storing and processing of personal data falls into two categories:

2.1 Business Management

This includes all data and systems that are used to manage and monitor the services that we provide, and includes **audit data**[1]

Where a specific requirement to gather **personal** data exists, which cannot be supported by a mainstream Trust Patient System, it will be permissible to gather that data on an "in-house or a 3rd party database system" providing the following procedure is strictly adhered to:

1. Approval in advance from the Trust Senior Information Risk Owner (SIRO) - through the Information Governance, Caldicott & SIRO Support (IGC&SS) Team - must be sought on the proposed collection, storage and use of data; some existing Information Assets may require additional security measures

2. The Trust Head of Information Governance | DPO will keep a record of the Information Asset on a central register. Users must supply the following data for consideration by the Information Management Systems (Registration) Team. An Information Management Systems (Registration) Proforma is provided at Appendix 1 for that purpose

    - Named individual as Information Asset Owner (IAO)
    - Named individual as Custodian or Information Asset Administrator (IAA) for the Asset
    - List of key demographic data items being recorded – these should always be *de minimus*
    - The source of each data item
    - Any parties to whom the data may be legally disclosed

3. The Information Services/Clinical Audit departments may necessarily be involved with the creation and safe output of any such Databases

[1] Where data are downloaded from one of the Trust's main Patient Management Systems or where they are entered manually into a data processing application such as MSAccess, MSExcel or similar, **strictly for Audit purposes** - and those data are the minimum required (Caldicott, et al. 2013) - then there would be no requirement to submit an application form in accordance with this policy. The Caldicott Guardian will expect that those data, in these cases, are 'looked after' during their use, and disposed of when necessary, in accordance with either local or Trust's Records Management Policies.

4. The data will normally reside on a Network Data Store and access to that data controlled by user name and password. Any other storage medium must have Caldicott and/or SIRO approval

5. An appropriate Risk Assessment will be carried out by the IAO and the IGC&SS Team

6. Whenever possible, the data will be adequately anonymised

7. In exceptional and authorised circumstances, if it is necessary to keep the data on a Trust supported Laptop or Personal Computer, then:

   - The Laptop or Personal Computer will have the Trust preferred encryption software installed so as to protect the data thereon, for example in case of theft

   - Procedures for making security backup copies of the data will be implemented

8. In all cases, data may **not** be copied on to any PC or computer system not belonging to the Trust without the expressed consent of the Caldicott Guardian through the registration process as managed by the IGC&SS Team.

2.2 Clinical Management

This includes all data and systems used for Clinical Management and/or the treatment of patients and staff and includes any system contributing to an Electronic Patient or Staff Record.

It is the Trusts' policy to only procure and use proven systems from reputable suppliers, for the storing and processing of personal data for clinical management and/or the treatment of patients. All such systems must be approved by the Clinical Safety Officer (CSO)[2] through the Trusts IGC&SS Team.

Mainstream Trust Patient Systems are subject to the control requirements detailed in NHS Digitals: Data Security and Protection (DSP) Toolkit.

3. EQUALITY IMPACT ASSESSMENT

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Fair Treatment For All Policy (CORP/EMP 4).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 5).

[2] The CSO acts in compliance with DSCN 14 & 18/2009

4. DUTIES AND RESPONSIBILITIES

The Trust Senior Information Risk Owner (SIRO) has overall responsibility for the registration, security, management and sign-off of all Trust Information Assets.

Information Asset Owners (IAOs) are responsible to the Trust SIRO for the implementation of the Trust's Information Systems Access Control Policy Statement. Specifically they are responsible for:

- *the management and control of all Users who have access rights to the system/s for which they have responsibility.*
- *ensuring their responsibilities are detailed in their personal job description*
- *liaising with the Trust Clinical Safety Officer[3] for any systems risk issues which might have any adverse or potentially adverse risks to patients or staff*

The main Trust Patient Clinical Systems are:

- *CaMIS Patient Administration System (PAS)*
- *Pathology*
- *PACS*
- *RIS*
- *Symphony ED*
- *Theatres (Blue Spear)*
- *Maternity (K2)*
- *GU Medicine*
- *JAC (Pharmacy)*
- *Sunquest ICE*
- *DBTH Clinical Portal*
- *TPP SystmONE*
- *Fresenius Renal*

Information Asset Administrators (IAAs) are responsible to their relevant IAO for the day to day access and management arrangements for their registered system. Specifically they are responsible for:

- *ensuring their responsibilities are detailed in their personal job description*
- *maintaining a control log of all Users and ex-Users.*
- *ensuring that all users are properly trained and have access to sufficient training materials and guidance to enable them to use their system efficiently and effectively.*
- *keeping a secure note of all Administration Usernames and Passwords within a sealed envelope which should be kept in a safe and recorded location, in case of an operational emergency.*

The Head of Information Governance/DPO is responsible for the coordinated registration process and associated registration database.

[3] DSCN 14 & 18 (2009)

5. PROCEDURE

Individuals must **not** undertake the development/use of any NEW systems for clinical management purposes until a **Data Privacy Impact Assessment** (DPIA) has been carried out by the IAO and Head of IG/DPO in conjunction with the Information Governance Committee.

This may necessarily include the completion of the NHSE DTAC (Digital Technology Assessment Criteria), which also includes a section on Clinical Safety.

The two standards issued by the NHS relating to digital clinical safety are:

- DCB0129 – ***Clinical Risk Management: its Application in the Manufacture of Health IT Systems.*** This standard is designed to help manufacturers of health IT software evidence the clinical safety of their products. Any health organisation looking to implement a solution can request, and should be provided with, this documentation.

- DCB0160 – ***Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems***. This standard is designed to help health and care organisations assure the clinical safety of their health IT software.

Information Management Systems used for clinical management and/or patient treatment, developed "in-house" or "externally", may not comply 'fully' with the terms of the UK GDPR and/or UK Data Protection Act 2018, or NHS Digital's Records Management Code of Practice 2016.

6. TRAINING AND SUPPORT

The IAO is responsible for ensuring that all users are properly trained and have access to sufficient training materials and guidance to enable them to use their system efficiently and effectively.

7. MONITORING COMPLIANCE

The Head of Information Governance is responsible for periodic monitoring and audit of the IMS Registration Process. Results will be presented to the Trust Information Governance Committee and then onto the Audit and Risk Committee (ARC) through their receipt and acknowledgement of the Information Governance Committee (IGC) Minutes and other papers.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
The System/Asset has formal 'signed' approval for use in the Trust The Asset must be recorded on the Information Asset central register	Trust Information Governance Committee	Twice Annually	Data Security and Protection (DSP) Toolkit reporting to the Trust Information Governance Group

The Asset has named individuals acting as Information Asset Owner (IAO) and Asset Administrator (IAA) Any parties to whom the data may legally be disclosed are 'mapped' The data will normally reside on a Network Data Store and access to that data controlled by username and password. Approval of any associated DPIAs or DTACs			

8. OTHER ASSOCIATED TRUST PROCEDURAL DOCUMENTS

CORP/ICT - Information, Communication and Technology (ICT) Section

CORP/ICT 2 - Information Management and Technology (IM&T) Security Policy

CORP/ICT 7 - Data Protection Policy

CORP/ICT 9 - Information Governance Policy

CORP/ICT 10 - Confidentiality - Code of Conduct

CORP/ICT 11 - Information and Communications Technology (ICT) Business Continuity Policy

CORP/ICT 14 - Information Records Management - Code of Practice

CORP/ICT 15 - Freedom of Information (FOI) Policy

CORP/ICT 16 - Information Governance Strategy

CORP/ICT 20 - Bulk Data Transfer Guidelines

CORP/ICT 21 - Information Risk Management Policy

CORP/ICT 22 – 3rd Party Access to the Doncaster and Teaching Hospitals NHS Foundation Trust's Network and Core Patient Systems

CORP/ICT 23 - Data Quality Policy

CORP/EMP 4 – Fair Treatment for All

CORP/EMP 27 – Equality Analysis Policy

9. DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

10. REFERENCES

DSCNs 14 and 18 of 2009

APPENDIX 1 – INFORMATION MANAGEMENT SYSTEM (IMS) REGISTRATION PROFORMA

Please send this completed sheet 'only' to the Trust Data Protection Officer: dbth.dpo@nhs.net

Division or Department:

Name/Subject of Information Asset **Information Asset Owner** (IAO)

……

What you need to tell us and why:

Note: The subject matter and disclosures you specify at Appendix B, MUST comply with Trust's Notification to the Information Commissioner under GDPR, the Data Protection Act 2018, and the Caldicott Principles listed below; additionally as the IAO and IAA, you should understand that by being a signatory to this registration that you are affirming the highest standard of use:

- Ensure that there is a lawful basis for processing (as in GDPR Article 9 2 (h))
- Justify the purpose(s)
- Don't use patient-identifiable information unless it is absolutely necessary
- Use the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict 'need to know' basis
- Everyone should be aware of their responsibilities
- Understand and comply with the Law
- To share or not to share

Do you need to carry out a Data Protection Impact Assessment (DPIA) for Personal Data Management? Yes ☐ No ☐

Where is the Data to be securely Held/Stored?

Trust Network Data Store ☐
(This will be the norm, except in exceptional circumstances, as it would be if through one of the Trust media below)

Other (You must give details here)

Encrypted Trust PC ☐ Encrypted Trust Lap Top ☐

What is the Database to be used for: -

(a) Business Management Yes ☐ No ☐

(b) Clinical Management Yes ☐ No ☐

If (b), Is the system used to support Clinical decision making Yes ☐ No ☐
If Yes, please give details:

Your Signature Block as **IAO**, confirms that **you and your Information Asset Administrator (IAA)** if there is one, have **read and understood** the Information Management Systems (Registration) Policy

Signature …… *Dated* ……

Name, Job Role

Tel:

APPENDIX 2 – DISCLOSURE DETAILS FORM

Disclosure details – Must be completed		
Who are you intending to 'legally' share the data with (data mapping), should there be any 'personal' data involved?		
List the 'justified'[4] personal demographic data items first, and then the main subject headings (only) for the non-demographic data (Printed lists may be attached instead)	**CaMIS PAS/ ODBC Linked** (Tick)	**Source of all other data**

Please ensure that any data collected is in accordance with the trust Privacy Notices and that there is therefore a 'legal basis' for the data processing/sharing.

Where personal data are intended for an external entity (such as a National Registry) then you must have the patients' explicit and documented consent for audit purposes, and when appropriate refer them to the Trust Privacy Notices.

[4] Justification for storing or sharing 'personal data' should be i.a.w. EU GDPR and the UK Data Protection Act 2018

APPENDIX 3 - INFORMATION GOVERNANCE AND REGISTRATION AUTHORITY CONSIDERATIONS IN ANY IT SERVICES/INFORMATION SYSTEM PROJECT

Policy check at a Glance

Information Asset Registration Matrix	New Trust Core System Yes, No or N/A	In-House Division or Departmental System/Database Yes, No or N/A	3rd Party, Divisional, or Departmental System/Database Yes, No or N/A
Project Agreed – including Funding and Staffing arrangements - at an appropriate and authorised Trust Level			
Information Asset Owner (IAO) and Administrator (IAA) identified and appointed; some additional IG/RA training may be required at this point			
IG and RA Risks identified and mitigated (<5) by Head of IG and system IAO/IAA (Appendix 3 Completed)			
Is a Data Privacy Impact Assessment (DPIA) required as at Appendix 4?			
Is a Privacy Notice (PN) required?			
Is a Digital Technology Assessment Criteria (DTAC) required where advice and assistance can be sought from the IGC&SS Team			
Is Clinical Safety Reporting advice required from the Trust Chief Nursing Information Officer			
Project Registered with Head of Information Governance | Trust DPO			
IG Committee sign-off (where necessary)			

Further Considerations and Checks

- Early involvement of your IG Lead/Trust DPO
- Appointment of Divisional/Departmental leads as Information Asset Owners and Asset Administrators (IAO and IAA) to take responsibility in their specific areas
- Clarify roles and responsibilities
    - Consider who to include on project team – consider IAO, Trust IG Lead, RA manager, Clinical Governance Lead, Caldicott Guardian, Trust SIRO
    - IG Risks
- Include cost of IG, IT and RA elements etc. within project costs
- Refer to National Guidance including key websites
- SET IG Training
    - Departmental Induction
    - Annual staff IG Compliance
    - Enhanced RA training prior to issuing Smartcards
    - Use of Smartcards
- Printer Locations
    - Is it in a convenient place that suits the application?
    - Does it require a confidential location?
    - Do staff need, and indeed are they allowed to print?
- Consent **(**please consider a 'legal basis', rather than implied consent, as it might not be necessary under **GDPR Art 6 1 and Art 9 2)**
    - Provide links to National Guidance
- Information Sharing Protocols/Agreements
    - Protocols developed and/or reviewed and that are in place
- Registration Authority (RA)
    - RA manager involvement
    - Refer to trust intranet website guidance on RA
    - Any need for HR (PoD) involvement
    - Determination and allocation of Position Based Access Control (PBAC) roles
    - Agents and Sponsors (sufficient resource, start soon enough)
    - Arrangements for issuing Smartcards including identity and DBS checks prior to new starters arrival
    - Smartcards for non-NHS staff
    - Infrastructure – card readers
    - Arrangements for Fallback cards
- Training environment with dummy data
    - Training data
- Testing
    - Testing data
- Data Migration
    - Initial DQ review
    - Resource allocation
    - Start early
    - DQ Tools
    - Use of DQ facilitators

  - Data Mapping decisions
  - Training on data quality for users (end users and specialists)
  - Clinical Coding knowledge and training?
  - Effective and validated data recovery processes
  - Alleged breaches of security investigated promptly and efficiently (within 72 hours overall)
- Communications
  - staff
  - patients
  - public
  - Divisions/Directorates
  - JSCC
  - Union groups
  - Professional committees
  - Team brief cascades
  - leaflets that meet guidance and audience needs
  - trust website and or Intranet/Extranet
- Document IG Benefits
  - IG enablers vs benefits
  - Methods of measuring IG benefits
- Contingency Planning
  - Involvement of Clinical Governance Leads
  - Business Continuity Plans
  - Data recovery
  - Guidance e.g. OGC Guide on Contingency Planning
- Process Change and Private Areas
  - Process mapping to include good IG practices and who sees what data
- Review implementation of IG standards after go live
- Sealed envelope
  - Consider in context of particular project
  - Reflect in communications
- Audit and Monitoring arrangements

APPENDIX 4 – DPIA Mask for completion

To be held as a separate document on the policy management page of the Trust extranet in due course. In the interim, please contact The IGC&SS Team here: dbth.dpo@nhs.net for the latest version copy

APPENDIX 5 - EQUALITY IMPACT ASSESSMENT – PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Division/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Information Management Systems (Registration) Policy – CORP/ICT 3 v.6	Digital Transformation Directorate	Roy Underwood	Existing Policy	January 2024

1) Who is responsible for this policy? Name of Division/Directorate: Digital Transformation Directorate

2) Describe the purpose of the service / function / policy / project/ strategy? To identify, authorise and to operate safely and securely all trust information assets

3) Are there any associated objectives? Data Protection Act 2018/GDPR/DH Records Management Code of Practice

4) What factors contribute or detract from achieving intended outcomes? IG Training

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? NO

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation]

6) Is there any scope for new measures which would promote equality? NO

7) Are any of the following groups adversely affected by the policy? NO

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form in Appendix 4

Date for next review: January 2027

Checked by: **Date:**