Shropshire Community Health
NHS Trust

National Data Opt-Out Policy

Controlled document

This document is uncontrolled when downloaded or printed.

Author(s)
Owner(s)
	Author: Gill Richards, Head of Information Governance/DPO
	Owner: Shelley Ramtuhul, Director of Governance/SIRO

Version No.	Version 2.1
Approval Date	June 2023
Review Date	June 2026

Document Details		
Title		National Data Opt-Out Policy
Trust Ref No		
Local Ref (optional)		
Main points the document covers		National Data Opt-Out Compliance
Who is the document aimed at?		This policy is aimed at all staff
Author		Head of Information Governance/Data Protection Officer
Approval process		
Who has been consulted in the development of this policy?		Data Security and Protection Assurance Group
Approved by (Committee/Director)		Data security and protection security group (DSPAG) Chaired by Director of Governance/Senior Information Risk Owner (SIRO)
Approval Date		16 June 2023
Initial Equality Impact Screening		
Full Equality Impact Assessment		
Lead Director		Director of Governance
Category		General
Subcategory		Information Governance
Review date		June 2026
Distribution		
Who the policy will be distributed to		The Head of IG will submit this document to the Risk Management Team for publication on the Trust Websites The IG Team will notify all Data Protection Liaison Officers (DPLOs) of the publication of this policy
Method		Websites and email
Keywords		PID; personal; identifiable; data; PII; information; person; confidential; sensitive
Document Links		
Required by CQC		Yes – Well Led
Other		
Amendments History		
No	Date	Amendment

1	May 2022	New policy created in line with National Data Opt-Out (NDOO) compliance.
2	April 2023	Update IG Manager to Head of IG, Director of Finance to Director of Governance
3		
4		
5		

This copy is uncontrolled unless printed on ‘Controlled’ paper.

Contents

1 Policy statement

1.1 Shropshire Community Health NHS Trust (hereafter the Trust) is committed to ensuring that all personal data we process, including that of our staff and colleagues, patients and service users, is managed appropriately and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "DP legislation").

1.2 Patients and staff trust us to take care of their personal data and will build productive relationships with us based on this trust.

1.3 This policy complies with our obligation in DP legislation to have an appropriate policy document in place where we are processing special category personal data for the purpose of employment obligations and substantial public interest reasons (see Article 9 of UK GDPR and Section 10 and Schedule 1 of the DPA 2018).

1.4 This policy complies with our obligation in the NHS National Data Opt-Out Operational Policy.

1.5 Negligent or malicious non-compliance with this policy may be dealt with through the disciplinary process.

2 Related documents

Policies can be found in Policies Library on Public Website and Staff Zone

- Information Security Policy
- Information Asset Register
- Records and Document Management Policy
- Information Risk Policy
- Registration Authority Policy
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright Designs and Patents Act
- Information Governance Procedures

This document includes links to guidance published by the UK Information Commissioner's Office (ICO) and by the European Data Protection Board (EDPB).

3 Purpose

3.1 This policy describes the plan of action that will be adopted to ensure that Shropshire Community Health NHS Trust meets its legal obligations under the data protection legislation and the NHS National Data Opt-Out Operational Policy here: National data opt-out operational policy guidance document - NHS Digital

3.2 The national data opt-out implements the opt-out model proposed by the National Data Guardian, as accepted by the Government and directed by the Department of Health and Social Care.

4 Scope

4.1 This Policy entails confidential patient information used for purposes beyond their individual care and treatment - for research and planning.

4.2 Any use or disclosure of confidential patient information for research and planning must be for the purpose of improving or benefitting health and care.

4.3 The National Data Opt-Out does not apply to information that is anonymised in line with the Information Commissioner's Office (ICO) Anonymisation: managing data protection risk code of practice (ico.org.uk)

4.4 Once compliant, confidential patient information must not be used or disclosed before it has been assessed and national data opt-outs applied when necessary.

5 Applicability

5.1 All staff that are required to work within the organisation, employed and non-employed, must adhere to this policy and associated policies. Including, but not limited to:

- Employed staff (including Bank staff)
- Volunteers
- Student Placements
- Medical Placements
- Allied Healthcare Placements
- Locums
- Agency
- Temporary and Fixed Term contracts
- Third Party Suppliers

6 Responsibilities

6.1 The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

Under the data protection legislation, the Trust is required to demonstrate that it has an information governance framework supported by the following roles:

6.2 The **Board** provides leadership on the management of risk and ensures the approach to risk management is consistently applied as well as determining the information risk appetite for the Trust. The Board is also responsible for setting the Trust's Risk Appetite regarding information security.

6.3 The **Senior Information Risk Owner (SIRO)** is the Board's executive level delegate responsible for risk management including oversight of data protection and other aspects of information governance. The role of the SIRO is to understand how the strategic business goals of the organisation may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board, including internal discussions, and will provide written advice to the Accountable Officer on the content of the annual Statement of Internal Control (SIC) with regards to information risk. The SIRO will advise the Chief Executive and the Board on information risk management strategies, provide periodic reports and briefing on risk management assurance and ensure that key risks are appropriately logged on the corporate risk register.

6.4 The **Chief Executive** is the Accountable Officer and has overall responsibility for ensuring our compliance with this policy and with Data Protection legislation. They have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. The organisation will set out a line of accountability, responsibility, and direction in accordance with the guidance set out in the Data Security and Protection Toolkit (DSPT) Standard 1 Personal Confidential Data, example diagram given below.

6.5 The **Chief Information Officer (CIO)** is an executive within the organisation that oversees the operation of the information technology department and consults with other personnel on technology-related needs and purchasing decisions. The CIO is the Head of Digital Services.

6.6 The **Caldicott Guardian (CG)** has responsibility for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. For any patient confidentiality issues the first point of contact should be the CG. The CG is also the designated **Privacy Officer.**

6.7 The **Chief Clinical Information Officer (CCIO)** is an executive within the organisation who is involved in change management, ensuring clinical adoption and engagement in the use of technology, supporting clinical process redesign in a digital world, providing clinical focus to ICT projects that will ensure the needs of the business are met with regards to patient care. The CCIO is the Medical Director/Caldicott Guardian.

6.8 The **Data Protection Officer (DPO)** has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for escalation as appropriate. The DPO is responsible for challenging and advising the Board on data protection to ensure that the Trust remains compliant.

6.9 The role of the **Information Asset Owner (IAO)** will be assigned to staff that hold the position of Deputy/Associate Director, Head of Department, Service Delivery Group Manager. The IAOs will be accountable to the Senior Information Risk Owner SIRO); and will have delegated responsibility from the SIRO to oversee and support the information risk management framework within their respective areas. The role will support the SIRO in fostering a culture that values, protects, and uses information for the benefit of patients, service users, employees and the Trust as whole.

6.10 The Information Asset Owner may nominate an **Information Asset Administrator (IAA)** and delegate the day-to-day responsibility of the information asset. The Information Asset Owner will nominate an appropriate person to undertake the role of **Data Protection Liaison Officer (DPLO)**.

6.11 **Data Protection Liaison Officers (DPLOs)** are responsible for providing administrative support to staff within the respective services/departments in the disclosure of personal data under the Data Protection legislation.

6.12 The **Head of Information Governance** is responsible for the day-to-day operational monitoring and compliance of information governance and information handling.

6.13 The **IT Service Manager** is responsible for the day-to-day management and operation of the corporate network infrastructure including the secure operation of the network, devices, connections, monitoring, protection, and controls.

6.14 A **Safe Haven function** will be established in all services, teams, and departments across the Trust. The IAOs will be responsible for identifying the safe haven(s) location and setting up the function in their respective areas; and the IAAs will be responsible for the day-to-day management and operation of safe-haven procedures. The safe haven environment will cover an agreed set of administrative procedures for the safe and secure handling of personal confidential information, such as reporting, handling Freedom of information and Subject access requests, dealing with requests from commissioners; and ensuring pseudonymisation and anonymisation is appropriately applied. The term "Safe Haven" means both a physical location within the organisation e.g., Trust premises or a virtual location e.g., MS Teams; where confidential information is both received and stored in a secure manner. A Register of Safe Havens will be held by the Head of Information Governance.

6.15 The **Head of Clinical Governance** is responsible for providing support to staff and managers who are responsible for information assets. They will provide support to the relevant groups and committees, including risk registers and monitoring service delivery risks.

6.16 The **Freedom of Information Manager** to ensure that the Trust complies with the Freedom of Information Act 2000 in processing Freedom of Information requests and the maintenance of a Publication Scheme. This role will manage the need to carefully balance the case for transparency and openness under the Freedom of Information Act against the data subject's right to privacy under the data protection legislation. Advising the organisation with regards to deciding whether the information can be released without infringing the UK GDPR and DPA 2018 data protection principles.

6.17 **All Line Managers** are responsible for ensuring that staff with responsibilities set out in this policy can undertake the role sufficiently, including training, to meet the organisation's obligations under the Data Protection legislation.

6.18 **All Staff** are responsible for upholding Data Protection requirements, including identifying and managing risk, and understanding/complying with relevant policies and procedures for handling personal data appropriate to their role. Staff must immediately report any event or breach affecting personal data held by the organisation to their Line Manager.

7 National Data Opt-Out Compliance

7.1 The National Data Opt-Out (NDOO) was introduced on 25 May 2018, enabling patients to opt-out from the use of their confidential patient information being used for research and planning, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

7.2 The Trust is compliant with the National Opt-Out Programme and has a process in place to receive requests for information. We will always apply the National Data Opt-Out operational guidance in respect of all personal data processed by the Trust, including personal data relating to all staff as set out in the Applicability section of this document. Staff that are involved in planning and research can contact the IG Team for advice and support to activate this process. The Standard Operating Procedure can be found on the Staff Zone. Further national details can be found here: National Opt-Out Programme

7.3 We will always comply with the National Data Opt-Out operational policy guidance as set out by NHS Digital here: National data opt-out operational policy guidance document - NHS Digital

7.4

7.5 Accountability requires the Trust to take responsibility for what we do with personal data and how we comply with the other principles. There must also be appropriate measures and records in place to be able to demonstrate compliance.

7.6 The Head of Information Governance and the Information Programme Manager are responsible for working with service/department managers to develop an electronic record e.g., register, that details each use or sharing of personal information, including the legal basis of the processing and if applicable, whether the National Data Opt-Out (NDOO) has been applied to any sharing of the data for secondary purposes.

7.7 We will always consider and apply the principles alongside existing data protection legislation, other laws, and best practice. These include data protection legislation and the Common Law Duty of Confidentiality (CLDC), Human Rights 1998, and all relevant Codes of Practice such as the DHSC and NHS Digital codes of confidentiality and best practice, for example The 8 Caldicott Principles as set out below:

1. Justify the purpose(s) for using confidential information.
2. Use confidential information only when it is necessary.
3. Use the minimum necessary confidential information.
4. Access to confidential information should be on a strict need-to-know basis.
5. Everyone with access to confidential information should be aware of their responsibilities.
6. Comply with the law.
7. The duty to share information for individual care is as important as the duty to protect patient confidentiality.
8. Inform patients and service users about how their confidential information is used.

8 Data Protection Compliance

8.1 We will ensure that we have a lawful basis for processing the data for the purpose of planning and research and record the legal basis on our Register of Processing Activity (ROPA).

8.2 We will comply with the data protection legislation as set out in the Trust's Data Protection Policy here: Data Protection Policy

8.3 All staff in the Trust who have responsibilities as set out in Section 6 of this document will adhere to this policy and support and guide others in processing information and managing information assets.

9 Retention of Personal Data

9.1 The Trust will apply the Records Management Code of Practice to new systems and business processes, through consultation with the Data Protection Officer, with regards to existing systems, and the acquisition and development of new information systems and on proposals for significant new business processes and change.

9.2 Staff should refer to the Trust's Records & Document Management Policy.

9.3 In 2011 NHS organisations were required to complete a data flow's transition and are now required to follow the NHS Digital and NHS England guidance, further information on the key points can be found at:

- NHS England s251 support for commissioning (https://www.england.nhs.uk/ig/in-val/)

- Safe Havens (https://www.digital.nhs.uk)
- Data Collections and data sets (https://www.digital.nhs.uk/data-and-information/datacollections-and-data-sets)
- Reference to Section 251: Control of patient information can be found under the legislation for the NHS Act 2006 at: http://www.legislation.gov.uk/ukpga/2006/41/section/251

Also see relevant ICO Guidance.

10 Training, Learning, Advice and Guidance

10.1 In addition to mandatory training all staff that undertake a role as set out in the Information Governance suite of policies under Roles and Responsibilities, will be required to complete appropriate role-based training, conferences, webinars, development, and specialist training as identified in the annual Learning Needs Analysis (LNA).

10.2 Staff will be required to seek appropriate advice, guidance, and support from the nominated Information Asset Owners (IAO) and/or the Information Asset Administrators, or other roles defined in the related suite of policies. Staff will have a good understanding of the compliance requirements as set out in national guidance, legislation and local policies and procedures, such as technical and organisational data security and protection measures.

11 Data Security Incidents

11.1 Any security incidents which may impact on the confidentiality, integrity or availability of personal data held by the organisation and must be reported immediately to the Data Protection Officer via the Trust’s Incident Reporting system Datix. Such events could include Loss of records, laptops or media containing personal data Unauthorised access to information systems containing personal data Access of personal data with no justifiable business need Personal data being misdirected to an incorrect recipient Loss of access to systems containing personal data All reported incidents will be recorded to ensure appropriate mitigation measures are in place and to identify lessons or necessary improvements.

11.2 The Data Protection Officer will consider whether the incident meets the UK GDPR and DPA 2018 definition of a “personal data breach” which presents a risk to individuals. He/she will present a report to the Senior Information Risk Owner including a recommendation on whether to report the matter to the Information Commissioner’s Office.

11.3 If the Senior Information Risk Owner decides that an incident constitutes a reportable data breach, the Data Protection Officer will report the incident to the Information Commissioner's Office (ICO) and liaise as appropriate.

11.4 If a data breach presents a high risk to the data subjects, the Data Protection Officer will ensure that they are also notified of the breach.

11.5 The Trust takes any data breach seriously. Any breach of the Data Protection Act 2018 constitutes a serious disciplinary offence. All breaches of Information Security, including near miss events, must be communicated to the relevant Information Asset Owner (IAO) and to the SIRO".

For further detail see the Personal Data Incident and Breach Reporting Procedure: European Data Protection Board Guidelines on Personal Data Breach Reporting and relevant ICO Guidance

12 Privacy Notice and Fair Processing

12.1 The UK GDPR requires that data controllers provide certain information to people whose data they hold and use.

12.2 This is known as a Privacy Notice (PN). The Trust shall provide PNs to all patients and all Employees, identifying who the data controller is, including contact details for the DPO. The PN should also explain the purposes for which personal data is collected and used, how the data is used and disclosed, how long it is kept, and the controller's legal basis for processing.

12.3 Statement of Fair Processing/PN will also be provided on the Trust's website. This reflects the requirement for a Statement of Fair Processing set out in the recommendations of the Caldicott Review.

13 Network and Information Systems Regulation (NISR)

13.1 The Trust applies The Networks and Information Systems Regulation (NISR) to all operations. The NISR aims to raise the levels of overall security and resilience of network and information systems for Operators of Essential Services across the UK and defines a set of principles used to guide decision-making. These principles fall under four main objectives:

- **Managing the Security Risks:** by ensuring appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services.
- **Protecting Against Cyber Attacks:** by ensuring proportionate security measures are in place to protect essential services and systems from Cyber-attack.
- **Detecting Cyber Security Events:** by ensuring security defences remain effective and detecting Cyber Security events affecting, or with the potential to affect, essential services.

- **Response and Recovery Planning:** having capabilities to minimise the impact of a Cyber Security incident on the delivery of essential services including the restoration of those services where necessary.

14 Contact

Any questions about this policy should be directed to:

Data Protection Officer, Shropshire Community Health NHS Trust,
William Farr House, Mytton Oak Road, Shrewsbury SY3 8XL

Email : shropcom.dataprotection@nhs.net

Tel : 01743 277500 Trust main switchboard

15 Review and Maintenance

This Policy shall be reviewed every two years or in response to significant changes due to security incidents, variations of law and/or changes to organisational or technical infrastructure'.

This Policy is authored by the Head of Information Governance/DPO and maintained by the Director of Governance on behalf of the Board. Questions relating to its content or application should be addressed to the Trust see contacts section above.

16 Appendix 1 - Data Security and Protection Assurance Framework

As set out in the Terms of Reference