journey to change

NHS
Tees, Esk and Wear Valleys
NHS Foundation Trust

Public – To be published on the Trust external website

Special category data policy

Ref: CORP-0070-v1

Status: Ratified
Document type: Policy

Contents

1 Introduction

In line with the legal requirements, we process special category (SC) data and criminal offence (CO) data in accordance with the requirements of Article 9 and 10 of the UK General Data Protection Regulation (UK GDPR) and Schedule 1 of the Data Protection Act 2018 (DPA 2018).

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document (APD) in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

Our Journey To Change sets out why we do what we do, the kind of organisation we want to become and the way we will get there by living our values, all of the time. To achieve this, the Trust has committed to three goals.

This policy supports all three goals of Our Journey To Change.

1.1 Strategic goal 1: To co-create a great experience for patients, carers and families

This policy gives transparency and accountability to all aspects of special category and criminal offence data that is processed within the Trust.

1.2 Strategic goal 2: To co-create a great experience for our colleagues

This policy ensures that all colleagues understand their role around the use and sharing of special category and criminal offence data that is shared, created or used by them. When staff understand their roles and their duties they can be confident that the actions that they take are consistent and defendable.

1.3 Strategic goal 3: To be a great partner

Information and its governance is a key communication tool and is strategic in assisting the Trust when it works with key partners either to improve services or to jointly care for patients. Working with other organisations and having robust agreements about the sharing of special category and criminal offence data enables information to support outstanding care and service delivery with our partners.

2 Why we need this policy

2.1 Purpose

This document explains our processing of special category and criminal offence data, and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notice.

2.2 Objectives

The policy sets out the Trust's requirements for compliance with its obligations under the Data Protection Act (DPA) 2018, the General Data Protection Regulation (UK GDPR), and associated laws and best practice and the Caldicott Principles.

3 Scope

3.1 What this policy applies to

Personal data is recorded information from which a living person can be identified, either from the data alone, or when combined with other data that is or may become available to the recipient of the data.

This policy covers:

- Special category and criminal offence personal data held and processed by the Trust.
- Personal data about service users, carers, applicants, students and staff (both present and past) and third parties. It includes pseudonymised data but not anonymised data.
- The Trust's requirements for data protection, whether it is the Data Controller or Data Processor, and where the Trust works in partnership with other organisation(s) as joint Data Controller, for example, to achieve seamless or integrated care for patients or service users.

This policy applies to:

- All personal data, whether held on-premise, cloud, on a portable device or by third parties. It applies to information held electronically and on paper.

3.2 Who this policy applies to

- All Trust employees, Non-Executive Directors, students, volunteers and contractors and third parties who work for or on behalf of the Trust and who have access to Trust information assets.

4 Roles and responsibilities

Role	Responsibility
Trust Board	• Sponsors of the Trust's Information Governance (IG) framework, taking into account legal and NHS requirements. • Ensuring sufficient resources are provided to support the requirements of the policy.
Audit and Risk Committee (ARC)	ARC reviews the establishment and maintenance of an effective system of integrated governance, organisational risk management and internal control to support the achievement of the organisation's Strategic Objectives, and specifically reviews the adequacy of: • the Trust's policies, processes and procedures to manage organisational risk and the internal control framework, including the design, implementation and effectiveness of those systems; • the policies for ensuring compliance with relevant regulatory, legal and code of conduct requirements.
Digital Performance and Assurance Group (DPAG)	• Ensuring processes are in place to address IG issues; develop and maintain policies, standards, procedures and guidance, co-ordinate and raise awareness of IG within the Trust. • Reporting on an exceptions basis to the Management Group on significant issues.
Digital and Data Management Meeting	The purpose of the the Information Meeting will act as an oversight sub group, approving papers that report into Digital Performance and Assurance Group and Digital Programme Board. Provide departmental leadership, direction and oversight of all aspects of the Digital and Data Services Department's delivery against the Digital & Data Journey to Change.
Information Governance Group (IGG)	The primary purpose of the group is to support the core business, strategies and services of the organisation by

	ensuring that information is accurate, dealt with legally, securely, efficiently, and assures the quality, confidentiality, integrity and availability of all information held by the Trust and partners on its behalf. The group does this by assuring the Trust of: • Compliance with the Data Security and Protection Toolkit. • Compliance with Data Protection Legislation. • Compliance with recommendations and actions arising from internal and external audit. • Effective Information Governance (IG) and Caldicott best practice within the organisation and promote learning and improvement.
Assistant Chief Executive - SIRO Medical Director – Caldicott Guardian	The Board members responsible for championing IG across the Trust; are the Trust's Caldicott Guardian and Senior Information Risk Owner (SIRO). The SIRO is the chair of the DPAG.
Head of Information Governance and Data Protection	• The senior manager responsible for IG and the Trust's nominated Data Protection Officer.
Information Governance team	• Coordinate Data Protection activity under Data Protection Act 2018 (DPA 2018); • Overseeing the policies and procedures required by DPA and subsequent regulations • Coordinate and approve Data Protection Impact Assessments • Maintaining the Trust's registration under the Act • Carrying out compliance checks on the trust's data usage • Carry out compliance checks against all staff access to personal information on a need to know basis • Overseeing the processing of Subject Access Requests • Maintaining the Trust's Data Protection Issues Log • Maintaining the Trust's Subject Access and Disclosure Log • Provision of information to staff on the requirements of the DPA • Ensuring that any staff with special responsibilities under DPA are kept up to date with developing requirements

	• Ensuring that any new systems containing personal data, or new users of existing systems, are introduced in accordance with the Trust's registration as a Data Controller
Information Asset Owners (IAOs) and Information Asset Administrators (IAAs)	• IAOs are members of staff senior enough to make decisions concerning a specific information asset at the highest level. • IAOs understands what information is held, added and removed, how information is moved, who has access and why. • IAOs support the SIRO and are central to managing information risk throughout the organisation; • IAAs support IAOs and undertake responsibility for information assets on a day to day basis.
Managers	On-going compliance by ensuring that the policy and its supporting standards and guidelines relating to IG are built into local processes.
All Trust staff	• Complying with this policy. • Ensuring that they understand their duties and obligations. • Undertaking training and awareness relevant to their role.

5 Policy

Under the Data Protection Act 2018, the Trust processes your data for the performance of a task carried out in the public interest and in exercising our official authority.

This means that it is necessary for us to process your data for those purposes. Additionally, other alternative conditions may be applicable where the above justification is not available for example, in the event of a life or death situation such as to prevent harm being caused by a patient or service user.

We have set out below a description of all the ways we use your personal data, and the legal bases we rely on to do so.

5.1 Processing special category data

Conditions for processing special category data are as follows:

- **Article 9(a)**: the data subject has given explicit consent.

- **Article 9(b)**: the processing is necessary for the purposes of exercising its obligations e.g.: employment.
- **Article 9(c)**: processing is necessary to protect the vital interests if the data subject e.g.: processing health information in a medical emergency.
- **Article 9(d)**: processing is carried out for a not-for-profit organization e.g.: union.
- **Article 9(e)**: the data has been made public by the data subject.
- **Article 9(f)**: for the establishment, exercise or defence of legal claims e.g.: litigation or employment tribunal.
- **Article 9(g)**: substantial public interest. If relying on substantial public interest then a condition of this is for the controller to have an appropriate policy document in place.
- **Article 9(h)**: the data is being processed for health and social care purposes.
- **Article 9(i)**: public interest in public health and is carried out under the supervision of a health professional.
- **Article 9(j)**: archiving, research and statistics.

We process criminal offence data under Article 10 of the GDPR. Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

5.2 Processing which requires an Appropriate Policy Document (APD)

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD.

This section of the policy is the APD for the Trust. It demonstrates that the processing of special category and criminal offence data based on these specific Schedule 1 conditions are compliant with the requirements of the GDPR Article 5 principles. Special category and criminal offence data is held in line with the Trust's Records Management Retention and Disposition Procedure.

5.3 Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, and trade union membership. Further information about this processing can be found in our Staff Privacy Notice.

We process the special category data about our patients that is necessary to fulfil our obligations as a health care provider. This may include data about patients who hold a Gender Recognition Certificate. Specific guidance for handling information and records relating to Trans patients, refer to the Minimum Standards for Clinical Record Keeping.

Our processing for reasons of substantial public interest relates to the data we receive or obtain to fulfil our statutory function as a health care provider. This may be health data,

evidence provided to us as part of a complaint or intelligence information we gather for our investigations. Further information about this processing can be found in our Privacy Notice on the Trust's external website.

We maintain a record of processing activities (ROPA) in accordance with Article 30 of the GDPR.

5.4 Schedule 1 conditions for processing

5.4.1 Special category data

We process special category data for the following purposes in Part 1 of Schedule 1:

- **Paragraph 1(1):** employment, social security and social protection.

We process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- **Paragraph 6(1) and (2)(a)**: statutory, etc. purposes
- **Paragraph 10(1)**: preventing or detecting unlawful acts
- **Paragraph 11(1) and (2)**: protecting the public against dishonesty
- **Paragraph 12(1) and (2)**: regulatory requirements relating to unlawful acts and dishonesty
- **Paragraph 24(1) and (2)**: disclosure to elected representatives

5.4.2 Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

- **Paragraph 1**: employment, social security and social protection
- **Paragraph 6(2)(a)**: statutory, etc. purposes

There are procedures for ensuring compliance with the principles.

5.5 Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer who reports directly to our highest management level.

- Implementing a 'data protection by design and default' approach to our activities.
- Maintaining a record of our processing activities.
- Adopting and implementing data protection policies and ensuring we have written contracts and information sharing agreements in place with our partner organisations and joint data controllers.
- Implementing appropriate technical and organisational security measures for the personal data we process.
- Carrying out data protection impact assessments for our high risk processing and implementing risk mitigation actions.

We regularly review our accountability measures and update or amend them when required.

5.5.1 Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and this policy document.

Our processing for purposes of substantial public interest is necessary for the exercise of a function conferred on the Trust by legislation.

Our processing for the purposes of employment relates to our obligations as an employer.

We also process special category personal data to comply with other obligations imposed on the Trust in its capacity as a public authority e.g. the Equality Act.

5.5.2 Principle (b): purpose limitation

We will process data for the purpose it was provided to us as a health care provider or employer.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose. We keep a record of all data sharing.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

5.5.3 Principle (c): data minimisation

We ensure personal data collected is not excessive. The information we process is necessary for and proportionate to our purposes as described within the related Data Protection Impact Assessment(s). Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

5.5.4 Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure

that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

5.5.5 Principle (e): storage limitation

All special category data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our retention schedule. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. The Trust adheres to the retention schedule specified within the NHSX Records Management Code of Practice 2021.

Records that may or may not be of use for an inquiry must be retained until there is clear instruction from the inquiry. There are currently three independent inquiries which have requested that large parts of the health and social care sector do not destroy any records that are, or may fall into the remit of the inquiry:

- The Infected Blood Inquiry - further information about the records required can be found on their website.
- UK COVID-19 Inquiry – this inquiry started in April 2021 and will examine, consider and report on preparations and the response to the pandemic in England, Wales, Scotland and Northern Ireland, up to and including the inquiry's formal setting-up date.

5.5.6 Principle (f): integrity and confidentiality (security)

This policy applies regardless of the media on which data is held. All data is managed in line with the Trust's Information Security and Risk Policy. Electronic systems and physical storage have appropriate access controls applied as per the Access to Information Systems Policy and Physical Security Policy. The systems we use to process personal data are auditable and allow us to erase or rectify personal data at any point in time where appropriate.

The Trust's data security and protection arrangements are declared annually via the NHSD data security and protection toolkit which is subject to external audit and scrutiny.

Our retention and disposal practices are set out in our retention and disposal policy available on the Trust's website.

5.6 Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our Trust Privacy Notice on our external website.

6 Definitions

Term	Definition
Confidentiality	Maintaining the intention/expectation to keep something secret or private
Disclosure	The act of making secret information known
Criminal Conviction or Offence Data	Article 10 GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'. Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.
DPIA	Data Protection Impact Assessment
DSPT	Data Security and Protection Toolkit - an online system which allows NHS organisations and partners to assess themselves against the Department of Health information governance standards.
GDPR	The General Data Protection Regulation (GDPR) is a European Union regulation on information privacy in the European union and the European Economic Area. As of 06 October 2022, the United Kingdom enacted its own law identical to the GDPR (UK GDPR).
Natural person	A natural person is an individual human being, distinguished from the broader category of a legal person, which may be a private (i.e., business entity or non-governmental organization) or public (i.e., government) organization
Privacy	A state of not being observed or disturbed by other people; being free from public attention
SAR	Subject Access Request

Special Category data	Special category data is defined at Article 9 GDPR as personal data revealing: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data for the purpose of uniquely identifying a natural person • Data concerning health or • Data concerning a natural person's sex life or sexual orientation.
UK GDPR	The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The UK GDPR sits alongside and amended version of the Data Protection Act 2018.

7 Related documents

Records Management – Retention and Disposition Procedure (CORP-0026-001)
Data Protection Impact Assessment Procedure (IT-0030-001)

8 How this policy will be implemented

- This policy will be published on both the staff intranet and Trust website.
- The line manager will disseminate this policy to all Trust employees through a line management briefing.

8.1 Implementation action plan

Activity	Expected outcome	Timescale	Responsibility	Means of verification/ measurement
Policy bulletin	Notification to all staff	Month of publication	Policy coordinator	Distribution list
Briefing article	Notification to all staff	Week of publication	Policy lead	Distribution list
SIRO bulletin article	Notification to all staff	Quarterly publication	Policy lead	Distribution list

8.2 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	Mandatory Data Security and Protection (IG) Training	1.5-2 hours	Annually

9 How the implementation of this policy will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Review of Data Protection Impact Assessments	Annually, Data Protection Officer	Information Governance Group
2	Review of Privacy Notices	Annually, Data Protection Officer	Information Governance Group

10 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	20 December 2023
Next review date	20 December 2026
This document replaces	N/A - new document
This document was approved by	Digital Performance and Assurance Group
This document was approved	06 September 2023
This document was ratified by	Management Group
This document was ratified	20 December 2023
An equality analysis was completed on this policy on	10 February 2023
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
1	20 Dec 2023	New document	Ratified

Appendix 1 - Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Information Governance
Title	Special Category Data Policy
Type	Policy
Geographical area covered	Trust-wide
Aims and objectives	This document explains our processing of special category and criminal offence data, and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018. In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement. The information supplements our privacy notice.
Start date of Equality Analysis Screening	10 February 2022
End date of Equality Analysis Screening	05 July 2022

Section 2	Impacts
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Service users, carers, applicants, students and staff (both present and past) and third parties about whom the Trust holds data.
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO**

	• **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed Forces** (includes serving armed forces personnel, reservists, veterans and their families **NO**
Describe any negative impacts	None
Describe any positive impacts	This policy gives transparency and accountability to all aspects of special category and criminal offence data that is processed within the Trust.

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	Data Protection Act (DPA) 2018, the General Data Protection Regulation (UK GDPR), associated laws and best practice and the Caldicott Principles.
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, describe the engagement and involvement that has taken place	This policy has undergone Trust-wide consultation. Trust staff comprise all protected characteristics.

If you answered No above, describe future plans that you may have to engage and involve people from different groups	

Section 4	Training needs
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	
Describe any training needs for patients	
Describe any training needs for contractors or other outside agencies	

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes / No / Not applicable	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Training**		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	
7.	**Implementation and monitoring**		

	Title of document being reviewed:	Yes / No / Not applicable	Comments
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
10.	**Publication**		
	Has the policy been reviewed for harm?	Yes	
	Does the document identify whether it is private or public?	Yes	
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	Not applicable	