Torbay and South Devon NHS
NHS Foundation Trust

Appropriate Policy Document (special category data)

Document Information

Date of Issue:	March 2021	**Next Review Date:**	April 2022
Version:	1.0	**Last Review Date:**	April 2021
Document Ref:	TSDFT Appropriate Policy Document		
Author:	Data Security and Protection Lead		
Directorate:	SDHIS		
Approval Route: Information Governance Steering Group the Audit and Assurance Committee			
Approved By:		**Date Approved:**	
Information Governance Steering Group		Via MSteams 23/04/2021	

Amendment History

Version	Status	Date	Reason for change	Authorised
0.1	Draft	01/03/2021	New document	Elaine Yersin
1.0	Final	23/04/2021	Ratified	IGSG

In the application of this policy Torbay and South Devon NHS Foundation Trust will not discriminate against any persons regardless of sex, race, colour, language, religion, political, or other opinion, national or social origin, association with national minority, property, birth, or other status as defined under Article 14, European Convention human Rights (ECHR) 1998, Race Relations (Amendment) Act 2000 and the Disability Discrimination (Amendment) Action 2005

Torbay and South Devon NHS
NHS Foundation Trust

Contents

Executive Summary

In line with the legal requirements, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('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.

This document explains our processing 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

Introduction 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.

This document also refers to Criminal conviction data

Criminal conviction 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.

Processing special category data

Conditions for processing special category data are listed below

Article 9 a: the data subject has given explicit consent

Article 9 b: the processing is necessary for the purposes of exercising its obligations

eg: employment

Article 9 c: processing is necessary to protect the vital interests if the data subject

eg: processing health information in a medical emergency

Article 9 d: processing is carried out for a not-for-profit organization

eg: 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

eg: 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.

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 ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the GDPR Article 5 principles. Special category and criminal offence data is held in line with the Trust's Retention and Disposal Policy.

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, photographs and their membership of any trade union. Further information about this processing can be found in our Privacy Notice

We process the special category data about our service users that is necessary to fulfil our obligations as a health and social care provider

Our processing for reasons of substantial public interest relates to the data we receive or obtain in order 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 our public website

We also maintain a record of our processing activities in accordance with Article 30 of the GDPR.

Schedule 1 conditions for processing

Special category data

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

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

  We process SC 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

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

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.

Taking a 'data protection by design and default' approach to our activities.

Maintaining documentation of our processing activities.

Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors.

Implementing appropriate security measures in relation to the personal data we process.

Carrying out data protection impact assessments for our high risk processing.

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

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 the 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.

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 will keep a record of all data sharing.

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

Principle (c): data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

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.

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. Our retention schedule is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)

Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures. Our electronic systems and physical storage have appropriate access controls applied. The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

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

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 public website

Responsibilities

The following roles are responsible for ensuring the accuracy of this document which is reviewed at Information Governance Steering Group

Trust Data Protection Officer (DPO)
Caldicott Guardian
Senior Information Risk Officer (SIRO)
Data Security and Protection Lead