Shropshire Community Health
NHS Trust

Standing Operating Procedure for

Handling Personal Confidential Data for Planning and Research Purposes:
National Data Opt-Out Compliance

Document Details		
Title		Handling Personal Confidential Data for Planning and Research Purposes: National Data Opt-Out Compliance
Trust Ref No		
Author		Gill Richards, Information Governance Manager
Related Trust Policy		National Data Opt-Out Policy
Approval process		
Approved by (Committee/Director)		Data Security and Protection Assurance Group (DSPAG) Director of Governance
Approval Date		
Review date		
Amendments History		
No	Date	Amendment
1		New Standard Operating Procedure (SOP)
2		
3		
4		
5		

Contents

1 Purpose

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.

The Trust must have a policy and procedures in place by the 31 July 2022 to ensure compliance.

The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning.

This document aims to provide practical local operational guidance for staff who are involved in managing requests to use and/or disclose Confidential Patient Information (CPI) for the purposes of planning and research.

This guidance should be read in conjunction with the Trust's National Data Opt-Out Policy here: [INSERT]

And the NHS national guidance published by NHS Digital here:
National data opt-out - NHS Digital

2 Background

The National Data Guardian's Review of Data Security, Consent and Opt-Outs proposed that:

"There should be a new consent/opt-out model to allow people to opt-out of their personal confidential data being used for purposes beyond their direct care."

The National Data Guardian review carefully considered the scope of the model including its limitation to purposes beyond individual care only and for it to be an opt-out rather than consent model:

"The Review was persuaded that the best balance between meeting these expectations and providing a choice to those who have concerns is achieved by providing an opt-out model. The review concluded that people should be made aware of the use of their data and the benefits; an opt-out model allows data to be used whilst allowing those who have concerns to opt out."

The review also acknowledged that:

"Whilst patients have a right under the NHS Constitution to request that their personal confidential data is not used beyond their direct care, there is currently no easy way for them to do that."

3 Introduction

This documented procedure is in place to support staff with what is allowed when using/disclosing patient data and when formal approval is required before data is used for another purpose or disclosed to a third party.

4 Scope

National data opt-outs are held on the NHS Spine against an individual's NHS number. If the use or disclosure of data needs to have national data opt-outs applied, the records for these patients must be removed from the data being used.

The opt-out only applies to confidential patient information - data that includes both:

- information that identifies or could be used to identify the patient
- details about their health or treatment

The national data opt-outs apply to:

- a disclosure when an organisation, for example a research body, confirms they have approval from the Confidentiality Advisory Group (CAG) for the disclosure of confidential patient information held by another organisation responsible for the data (the data controller) such as an NHS Trust.
- to information about an individual's health and adult social care provided in England;
- the processing of Confidential Patient Data for the purpose of planning and research;
- living patients;
- deceased patients.

The national data opt-outs **do not** apply to:

- the use of personal confidential data for the purposes of direct care;
- data that is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice (CoP) on Anonymisation; here: Anonymisation: managing data protection risk code of practice (ico.org.uk)
- workforce or staff data

5 Definitions

Confidential patient information" (CPI) is defined in Section 251 (11) of the National Health Service Act 2006. Broadly it is information that meets all of the following three requirements:

1. identifiable or likely identifiable (for example from other data likely to be in the possession of the data recipient); and
2. given in circumstances where the individual is owed an obligation of confidence; and
3. conveys some information about the physical or mental health or condition of an individual, a diagnosis of their condition; and/or their care or treatment.

Confidential also covers data which falls within the "special categories of personal data" under Article 9 of the General Data Protection Regulation (GDPR):

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- processing genetic data
- biometric data for the purpose of uniquely identifying a natural person
- data concerning health
- data concerning a natural person's sex life or sexual orientation

Note: some of the above data items will not be collected as part of the patient record.

The check for which patients have opted out is done through the **Messaging Exchange for Social Care and Health** (MESH).

It is important to note that research is different to clinical audit which is defined as:

> *"A quality improvement process that seeks to improve patient care and outcomes through systematic review of care against explicit criteria and the implementation of change"*
>
> *Clinical audit is about finding out if we are doing what we should be doing and implementing changes when a shortfall in the level of care is observed.*
>
> *It is different from research. Research defines what best practice is; audit involves collecting data to find out if best practice (as defined by research) is being followed".*

6 Responsibilities

- The Information Governance Manager and the Information Programme Manager are responsible for providing advice and guidance with regards to the application of this procedure;
- The Information Team is responsible for activating the formal process of the national data opt out via the Message Exchange for Social Care and Health (MESH);
- Information Asset Owners (IAOs) and Information Asset Administrators (IAAs) are responsible for data processing activity compliance with regards to the systems for which they have been identified as the "owner" and/or "administrator";

- The nominated lead for the planning or research data processing e.g. service manager or research team, must complete a Data Protection Impact Assessment (DPIA) that covers the data processing required to prepare a data set for disclosure with national opt-outs applied. The DPIA should be conducted in conjunction with the IAO and/or the IAA;
- The Information Governance Team is responsible for providing advice and support with regards to the data protection legislation;
- All staff are responsible for ensuring that the Individual rights of the Trust's patients are upheld under the data protection legislation;
- All staff are responsible for seeking advice and guidance with regards to this procedure.

7 Contacts

Please contact the following teams to discuss the intended use of data:

Information Governance Team: shropcom.dataprotection@nhs.net
Information Team: shropcom.info@nhs.net
Research Team: shropcom.research@nhs.net

8 Procedure

- The nominated lead for the research/planning data processing activity must make a request to conduct a Data Protection Impact Assessment (DPIA) via shropcom.dataprotection@nhs.net
- The request should include a description of the data processing requirements;
- The Information Governance Team to establish whether a full DPIA via the Information Sharing Gateway (ISG) is required or a mini DPIA;
- The DPIA must be conducted by the nominated lead and the Information Asset Administrator and other experts involved in the data processing;
- The DPIA must be reviewed by the Data Protection Officer and have Senior Officer sign-off by the SIRO or the Caldicott Guardian;
- Once the DPIA is approved and the national data opt-out applies contact the Information Team at shropcom.info@nhs.net to discuss and agree the extraction of a patient list. A list of patients can be provided from a range of sources with the expectation that most requests will utilise the Trust's Data Warehouse. The NHS Number is vital to this process;
- IAA to request a list of NHS Numbers to be taken from the records that are planned for disclosure, or the list of NHS numbers that might be disclosed during the time period of the cache;
- The Information Team submit a list of NHS numbers via the MESH, a list will be received back with the NHS numbers identified as opted-out removed from the file, and the NHS numbers that can be used remain as part of the file and for the data processing activity;

- IAA to work with the Information Team to compare the list of numbers that is returned with the original list and remove the records of any that no longer appear on the returned list from the data disclosure entirely, to create an updated set of data to be disclosed; Care must be taken to ensure accurate Version Control is applied appropriately, so that the correct final file for use is identified;
- The final cohort of patients must be sent securely to the nominated lead;
- The service to check for national data opt-outs is updated every 24 hrs which gives local organisations who access the service directly 20 days to process and disclose the data. Where a temporary cache of the data is held locally this must be updated at least every 7 days and in this case the organisation has 13 days to process and disclose the data;
- Patient lists must be held in a secure location and not retained for other purposes;
- Further advice and guidance from the IG Team can be sought accordingly;
- The nominated lead or the IAA must record the data flow on the Trust's Register of Processing Activity (ROPA);

Appendices:

Please see the following set of appendices at the end of this document that illustrate how to apply and document the NDOO

Appendix 1 Assess current and ongoing data disclosures
Appendix 2 Application of national data opt-outs within both data controller and or organisational boundaries
Appendix 3 Checklist

9 Training

The following staff who undertake a role related to planning, research and information assets will be asked to undertake relevant training:

- Information Asset Owners and/or Information Administrators
- Information Governance Team
- Information Team
- Research Team
- Strategy and Planning

Staff can access the NDOO training (approx. 45 mins) via a registration process, here: National Data Opt-Out Training - elearning for healthcare (e-lfh.org.uk)

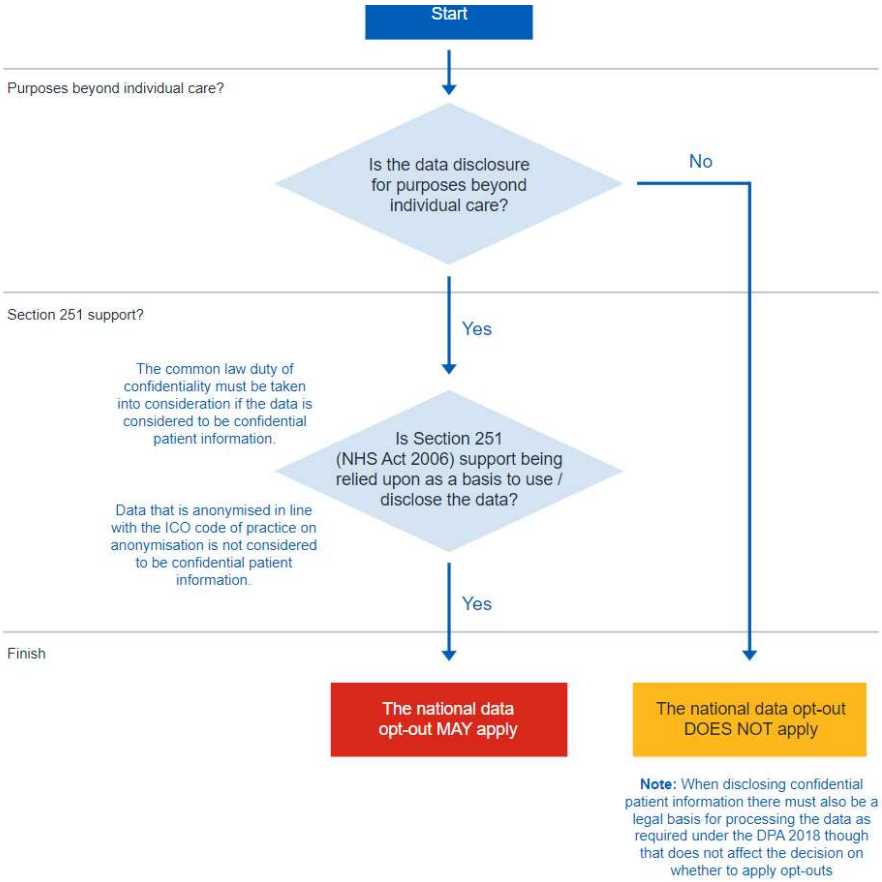
10 Monitoring

An ad-hoc audit will be undertaken annual to review the process and check compliance.

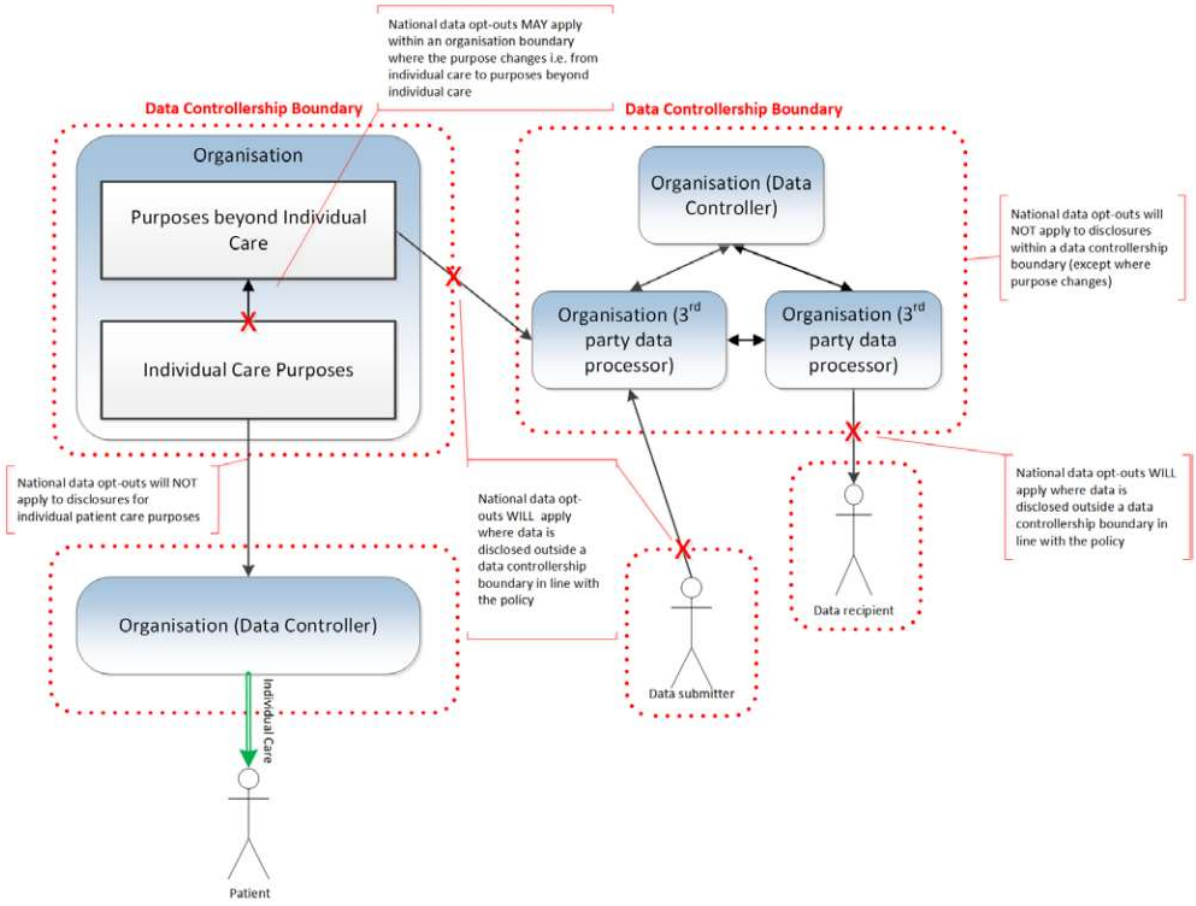
11 References

Full guidance about the National Opt-Out Programme can be found here: https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out

12 Appendix 1: Assess current and ongoing data disclosures



13 Appendix 2: Application of national data opt-outs within both data controller and organisational boundaries



14 Appendix 3: Checklist

Under the General Data Protection Regulation 2018 and the Data Protection Act 2018 we are required to document our data processing activity.

Use the checklist below to help you consider the purpose for the data processing and then record on the Trust's Register of Data Processing Activity (ROPA).

Advice can be sought from the IG Team, Information Team or the respective Information Asset Owner/Administrator.

Item	Consideration	Yes/No
1	Is the use or disclosure confidential patient information?	
2	Is the use or disclosure for individual care, research or planning?	
3	Do you have explicit consent for the use of disclosure?	
4	Is the disclosure for the purpose of monitoring and control of communicable disease or other risks to public health?	
5	Is the use or disclosure in the overriding public interest?	
6	Is the information being disclosed because of a legal requirement?	
7	Is the use or disclosure to a national or arms-length body?	
8	Is the use of disclosure to support payment and invoice validation?	
9	Is the legal basis for the use of disclosure of Section 251 approval?	