**National Data Opt-Out**

**Policy**

**Document Control:**

|  |  |
| --- | --- |
| **Version** | 1.2 |
| **Name and designation of policy author(s)** | Dr. Murugesh Velayudham  GP Senior Partner |
| **Ratified by** | Deepa Gnanasundaram |
| **Date Ratified** | Mar 2024 |
| **Responsible Committee/Officers** | Data Protection Officer/Data Processing Officer/  DS/AW/JM |
| **Date Issue** | 20/03/2024 |
| **Review Date** | July 2025 |
| **Intended Audience** | Practice Staff and Patients |
| **Links to other strategies, policies, procedures** | Access to Health Records Act 1990  SAR |

**Version History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author name and designation** | **Summary of main changes** |
| 20/03/2024 | **1.0** | **DS** |  |
| **July 2024** | **1.1** | **Deepa Gnanasundaram**  Practice manager | **Corrections to assigned SIRO** |
| **July2025** | **1.2** | **Deepa Gnanasundaram**  Practice manager |  |

**Table of Contents**

[**1.** **Introduction** 4](#_Toc130480412)

[**2.** **Purpose** 4](#_Toc130480413)

[**3.** **Scope** 4](#_Toc130480414)

[**4.** **Responsibilities** 5](#_Toc130480415)

[**5.** **Definitions** 5](#_Toc130480416)

[**6.** **Laws & Regulations** 7](#_Toc130480417)

[**7.** **National Data Opt Outs** 7](#_Toc130480418)

[7.1 Types of Data 7](#_Toc130480419)

[7.2 When an Opt Out Applies 8](#_Toc130480420)

[7.3 Patient Consent 9](#_Toc130480421)

[7.4 Geographic Coverage 10](#_Toc130480422)

[7.5 Deceased Patients 11](#_Toc130480423)

[7.6 National Patient Experience Surveys 11](#_Toc130480424)

[7.7 Age 11](#_Toc130480425)

[7.8 Population Screening Programmes 11](#_Toc130480426)

[7.9 Public Health England National Disease Registers 11](#_Toc130480427)

[7.10 Invoice Validation 11](#_Toc130480428)

[**8.** **Applying the National Data Opt Outs** 12](#_Toc130480429)

[**9.** **Review of the Policy** 12](#_Toc130480430)

# **Introduction**

* 1. The National Data Opt-Out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs. Organisations including the Storrsdale Medical Centre have been required to honour the National Data Opt-Out from 31 July 2022
  2. The National Data Opt-Out applies to the disclosure of confidential patient information for purposes beyond individual care across the health and adult social care system in England. The opt-out does not apply to data disclosed by providers of health and care services outside of England or to children’s social care services.
  3. The National Data Opt-Out is aligned with the authorisation used for sharing a patient’s data in accordance with the common law duty of confidentiality (CLDC). In broad terms the National Data Opt-Out applies unless there is a mandatory legal requirement or an overriding public interest for the data to be shared. The opt-out does not apply when the individual has consented to the sharing of their data or where the data is anonymised in line with the Information Commissioner’s Office (ICO) Anonymisation: managing data protection risk code of practice.
  4. Patients are able to opt out via <https://www.nhs.uk/your-nhs-data-matters/>. Patients can change their mind at any time. Their choice is held by NHS England (previously NHS Digital)

# **Purpose**

* 1. The purpose of this policy is to set out the way Storrsdale Medical Centre will comply with the National Data Opt-Out Programme. This will ensure that patients who have decided to opt out of having their identifiable data used for purposes beyond direct healthcare will have their informed decision complied with. When a preference to opt out has been made the Practice must ensure that the patient’s identifiable data is not used for the purposes of research or for activities which assist the Practice in managing its services. Any uses of patient identifiable data that is not directly for the provision of direct healthcare for the patient must be assessed to determine whether the National Data Opt-Out applies.

# **Scope**

* 1. This document applies to those members of staff that are directly employed by the Practice and for whom the Practice has legal responsibility, as well as any processors/contractors/sub-contractors/third parties processing Practice data or accessing systems, or anyone authorised to undertake work on behalf of the Practice. For those staff covered by a letter of authority/honorary contract or work experience, the organisation’s policies are also applicable whilst undertaking duties for or on behalf of the Practice.

# **Responsibilities**

* 1. **Senior Information Risk Owner** 
     1. The SIRO is accountable for information risk within the Practice. The Practice’s SIRO is is Deepa Gnanasundaram, the Practice Manager.
  2. **Caldicott Guardian**
     1. The Caldicott Guardian has responsibility for overseeing the implementation of the laws that govern personal information and ensuring that good practice in relation to access and reuse is implemented within the Practice.
     2. The Caldicott Guardian is the Practice champion in respect of the Caldicott Principles and as such is obligated to always make Caldicott decisions in the best interests of the patient. The Practice’s Caldicott Guardian is Deepa Gnanasundaram, the Practice Manager.
  3. **Data Protection Officer**
     1. The Data Protection Officer (DPO) has responsibility for informing and advising and monitoring compliance with data protection principles. The DPO for the Practice is held by the NHS Informatics Merseyside Data Protection Officer as a Service.

DPO: Head of Information Governance, NHS Informatics Merseyside, Information Governance Team, Hollins Park, Winwick, Warrington, WA2 8WA

* + 1. The DPO will:
* Provide advice to the Practice and its employees on compliance obligations with data protection law
* Advise on when data protection impact assessments are required
* Monitor compliance with data protection law and organisational policies in relation to data protection law
* Co-operate with, and be the first point of contact for the Information Commissioner
* Be the first point of contact within the organisation for all data protection matters
* Be available to be contacted directly by data subjects
* Take into account information risk when performing the above
  1. **All Staff**
     1. It is the responsibility of all staff to:
* Adhere to this policy
* To know where to access further support
* Complete annual Data Security Awareness mandatory training

# **Definitions**

* 1. **Anonymised Information**

Information about a patient’s health or care that is anonymised so that we can no longer identify them is not considered to be confidential information.

* 1. **Common Law Duty of Confidentiality**

The common law regarding information that is subject to a duty of confidence. This is sometimes termed the “common law duty of confidence”.

* 1. **Compliance**

Is used to refer to an organisation having assessed its data flows to determine whether they fall within the scope of National Data Opt-Out policy (as defined by this document), and applying the National Data Opt-Out as necessary to any flows that are within scope. An organisation may be compliant even if it is not applying the National Data Opt-Out where it does not have any data disclosures that need the opt-out to be applied. For example, where it is processing data for individual care only.

* 1. **Confidential Patient Information**

This is information which identifies a person and says something about their health, care or treatment. Patients would expect this information to be kept private. Information that only identifies them, like their name and address is not considered to be confidential patient information and may still be used if not combined with other data.

* 1. **Data Disclosure**

The term used to describe sharing of data in relation to the common law duty of confidentiality and is used to indicate the point at which the National Data Opt-Out must be applied.

* 1. **Individual Care**

Often referred to as ‘direct care’ where legally the sharing of data is based on implied consent, i.e. where the patient knows or would reasonably expect their data to be shared for their care and treatment.

* 1. **National Data Opt-Out**

The right for patients to withhold consent for their data to be used for research or planning of services.

* 1. **Purposes beyond Individual Care**

This is used to refer to all other uses of data outside an individual’s care and treatment. This is sometimes also referred to as “secondary uses”, “indirect care" or “other purposes”.

* 1. **Pseudonymised information**

Information about a patient’s health or care that is pseudonymised to an extent that it can no longer identify them in line with the Information Commissioners Code of Anonymisation is not considered to be confidential patient information.

1. **Laws & Regulations**
   1. This Nation Data Opt-Out Policy will ensure that the Practice complies with all relevant laws, legislation and regulation. This will include (but is not limited to):

* [Data Protection Act 2018](https://www.gov.uk/data-protection)
* [UK General Data Protection Regulations (UK GDPR)](https://www.legislation.gov.uk/eur/2016/679)
* [Health & Social Care Act 2012](https://www.legislation.gov.uk/ukpga/2012/7/contents)
* [Common Law Duty of Confidentiality](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care/hscic-guide-to-confidentiality-references/section-2)
* [Confidentiality: NHS Code of Practice](https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice)
* [Records Management Code of Practice for Health and Social Care 2021](https://transform.england.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf)

# **National Data Opt-Outs**

## **Types of Data**

* + 1. The National Data Opt-Out applies to “Confidential Patient Information” Confidential Patient Information is defined in Section 251 (11) of the National Health Service Act 2006. Broadly it is information that meets all of the following 3 requirements:
* identifiable or likely identifiable (for example from other data likely to be in the possession of the data recipient); and
* given in circumstances where the individual is owed an obligation of confidence; and
* 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.
  + 1. 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](https://ico.org.uk/media/for-%20organisations/documents/1061/anonymisation-code.pdf).
    2. The National Data Opt-Out is for patient data only and applies to confidential patient information - the National Data Opt-Out does not apply to workforce or staff data.

## **When an Opt-Out Applies**

|  |  |  |
| --- | --- | --- |
| **Legal basis in**  **common law** | **Opt-out applies** | **Comments** |
| Common Law  Consent (Implied): | **No** – out of  scope for the  National Data  Opt-Out | For common law purposes the sharing of information for direct or individual care purposes is on the basis of implied consent. This is out of scope for the National Data Opt-Out which only applies to purposes beyond individual care.  N.B. This is included in this table for completeness and to emphasise that implied consent can only be used when the surrounding circumstances mean that a patient knows, or would reasonably expect, that their data will be shared. In other words there should be ‘no surprises’ for the individual about who has had access to information about them where implied consent is relied upon. |
| Common Law Consent (Explicit) | **No** | In this case an individual has given their consent for a specific use of their data, for example consenting to participate in a research study. This would fall within the general exemption from the National Data Opt-Out. This rule applies even if the consent was given before the patient had set a National Data Opt-Out. |
| Mandatory Legal  Requirement | **No** | Where there is a legal requirement for the data disclosure that specifically sets aside the common law duty of confidentiality then the National Data Opt-Out will not apply. |
| Section 251  Regulation 2 – for  diagnosis and  treatment of cancer  Regulation 5 – for  the medical  purposes set out in  the schedule to the  regulations | **Yes** – in general  BUT there are some specific  exemptions | Data disclosure has Section 251 support obtained under regulation 2 or 5. This applies unless Confidentiality Advisory Group have advised:   1. that the National Data Opt-Out is overridden in the public interest (NB: This would be in exceptional circumstances only) or 2. a different opt-out can apply and the Section 251 decision-maker (Secretary of State for Health and Social Care or Health Research Authority) has agreed to this. For example data disclosures to Public Health England (PHE) for the National Cancer Register or the National Congenital Anomaly and Rare Diseases Register. |
| Section 251  Regulation 3 – for  communicable  diseases and other  risks to public health | **No** | Data disclosure under Regulation 3 of the Control of Patient Information Regulations 2002 is exempt from the National Data Opt-Out. |
| Patient identifiers are used for purposes of direct healthcare | **No** | In this case the patient opt out would not apply, GDPR Article 6(1) (e) and 9(2) (h) would be applied. |
| Patient information which is either anonymised or pseudonymised. And used for internal reporting, Data Quality and validation. | **No** | The National Data Opt-Out does not apply to information which does not uniquely identify a patient. |

## 

## **Patient Consent**

* + 1. The National Data Opt-Out does not apply where a patient has given their explicit consent to the specific use of their data. The use of consent for specific purposes is supported by the following from the National Data Guardian (NDG) review:
* “People should continue to be able to give their explicit consent separately if they wish, e.g. to be involved in research, as they do now. They should be able to do so regardless of whether they have opted out of their data being used for purposes beyond direct care. This should apply to patients’ decisions made both before and after the implementation of the new opt-out model”.
* As the NDG specified there is no dependency on the timing of when a person gave their consent for a specific disclosure of their data. A person may give consent for a specific purpose either before or after setting a National Data Opt-Out and this consent will constitute an exemption from the national data opt-out.

## **Geographic Coverage**

* + 1. The National Data Opt-Out relates to information about an individual’s health and adult social care provided in England.
    2. It does not apply to information about an individual’s health or care which is generated or processed outside of England including in home countries of the UK, such as Wales, Scotland, Northern Ireland, or the Isle of Man or Channel Islands
    3. Opt-outs offered in other home countries for example in Wales, Scotland, Northern Ireland, or the Isle of Man (IoM) or the Channel Islands do not apply in England – but they may be applied prior to receipt of any data in England.
    4. National Data Opt-Outs continue to apply until the individual proactively changes their opt-out preference, including where the individual subsequently moves away from England. For example, an individual moving from England to Wales who has a National Data Opt-Out but does not remove it when they move – their opt-out remains in place and is applied in line with this policy.

## **Interaction with other opt-outs**

* + 1. Prior to the launch of the National Data Opt-Out individuals could set two types of general opt-outs, via their GP practice:
* A **type 1** opt-out prevents an individual’s personally identifiable patient data being shared outside of their GP practice for purposes except their own care.
* A **type 2** opt-out prevents confidential patient information from being shared for research and planning.

Type 1 opt-outs will continue to be respected until the Department of Health and Social Care (DHSC) conducts a consultation with the NDG on their removal.

Type 2 opt outs have been replaced by the national data opt-out and are no longer valid. All type 2 opt- outs recorded in GP practices up to and including 11 October 2018 have been migrated to become national data opt-outs.

* + 1. NHS Digital (now NHS England) has written to inform people who previously registered a type 2 opt-out of this change. More information on the conversion of type 2 opt outs can be found on the NHS England website.
    2. Storrsdale Medical Centre as part of their compliance ran searches to identify if any patients had been codes with Type 2 on or after 11 October 2018 and contacted these patients to advise they would be required to register their objection via the ‘Your NHS Data Matters’ website (www.nhs.uk/your-nhs-data-matters)
    3. Other national and local opt-outs for specific purposes (for example summary care record opt out) remain in place and should continue to be applied, when appropriate, alongside the national data opt-out.

## **Deceased Patients**

* + 1. A National Data Opt-Out continues to be maintained and applied for an individual after they have died. Health and Adult Social Care organisations are expected to continue to apply opt-outs for deceased patients and their opt out will continue to be held on the Spine repository.

## **National Patient Experience Surveys**

* + 1. The National Data Opt-Out does not apply to the National Cancer Patient Experience Survey and CQC NHS Patient Survey Programme, both of which will continue to run unaffected under their current arrangements.
    2. These national surveys will continue to operate separate opt-out mechanisms and details of how to opt out of these surveys are provided locally.

## **Age**

* + 1. The opt out will only become an option when the patient has reached the age of 13, prior to that it will be down to the parent/guardian to decide on whether they wish for this data to be processed for purposes beyond patient care.

## **Population Screening Programmes**

* + 1. The National Data Opt-Out does not apply to disclosures of confidential patient information for the purpose of allowing participation in National Screening Programmes endorsed by the UK National Screening Committee.

## **Public Health England National Disease Registers**

* + 1. The National Data Opt-Out does not apply to Confidential Patient Information flowing to Public Health England (PHE) under the following approvals:
* National Cancer Register (PIAG 03(a)/2001);
* National Congenital Anomaly and Rare Diseases Register (CAG 10- 02(d)/2015).

## **Invoice Validation**

* + 1. In general, the National Data Opt-Out does not apply to data used for payment and invoice validation purposes. Specifically, the National Data Opt-Out does not apply to invoice validation for contracted and non-contracted activities, anonymised data should be used.

# **Applying the National Data Opt-Outs**

* + 1. If the practice wishes to run a search for identifiable patient data that would be used either internally by the practice or externally (shared out) for any reason beyond the patient's care and treatment and the National Data Opt-Out applies, this search should be run via EMIS Population Reporting.
    2. In the Search Builder function, the following should be completed:
* **Name:** A meaningful name for the search.
* **Description:** A description of the search.
* **Opt out:** Tick to apply the National Data Opt-out filter.
* **Based on:** Select required population.
* **Recipients:** A Recipient section is added when the National Data Opt-out.

filter is applied, complete as appropriate.

* + 1. The Practices must complete both the recipient and description boxes accurately, stating what the search is, what the results will be used for and if they are for internal Practice use or if being shared outside of the Practice who they are being shared with.
    2. The remainder of the search should be carried out as per normal procedures.

1. **Review of the Policy**
   1. This policy will be reviewed every year.