Text

Description automatically generated with medium confidence****

**National Data Opt-Out Policy**

**June 2023**

|  |  |
| --- | --- |
| **Authorship:** | Information Governance Delivery Manager – NHS Humber & North Yorkshire Integrated Care Board |
| **Committee Approved:** | SIRO & Information Governance Groups |
| **Approved date:** | June 2023 |
| **Equality Impact Assessment:** | April 2023 |
| **Target Audience:** | CB and its Committees and Sub-Committees, ICB Staff, agency and temporary staff & third parties under contract |
| **Policy Number:** | ICB41 |
| **Version Number:** | 1.0 |

**The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as ‘uncontrolled’ and as such may not necessarily contain the latest updates and amendments.**

**AMENDMENTS**

Amendments to the policy may be issued from time to time. A new amendment history will be issued with each change.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **New Version Number** | **Issued by** | **Nature of Amendment** | **Approving body** | **Approval date** | **Date published on website** |
| V1.0 | Executive Director of Corporate Affairs | New Policy for ICB | SIRO | 22.06.23 | 27.06.23 |

Contents

[1 Introduction 5](#_Toc132103172)

[2 Purpose 5](#_Toc132103173)

[3 Definition/ Explanation of Terms 5](#_Toc132103174)

[4 Scope of the Policy 6](#_Toc132103175)

[5 Duties/ Accountabilities and Responsibilities 6](#_Toc132103176)

[5.1 Duties within the organisation: 6](#_Toc132103177)

[5.2 Chief Executive 6](#_Toc132103178)

[5.3 Senior information risk owner (SIRO) 7](#_Toc132103179)

[5.4 Caldicott Guardian 7](#_Toc132103180)

[5.6 Information governance steering group 7](#_Toc132103181)

[5.7 Line Managers 7](#_Toc132103182)

[5.8 All staff: 7](#_Toc132103183)

[5.10 Responsibilities for approval 8](#_Toc132103184)

[6 Policy Document Requirements 8](#_Toc132103185)

[7 Consultation 10](#_Toc132103186)

[8 Training 10](#_Toc132103187)

[9 Monitoring Compliance 10](#_Toc132103188)

[10 Arrangements for Review 11](#_Toc132103189)

[11 Dissemination 11](#_Toc132103190)

[12 Associated Documentation 11](#_Toc132103191)

[13 References 11](#_Toc132103192)

[14 Appendices 11](#_Toc132103193)

[15 Impact Assessments 11](#_Toc132103194)

[15.1 Equality 11](#_Toc132103195)

[15.2 Bribery Act 2010 12](#_Toc132103196)

[15.3 General Data Protection Regulations (GDPR) 12](#_Toc132103197)

# Introduction

In response to the National Data Guardian (NDG) for Health and Care review of data security, consent and opt outs, the National Data Opt-Out Programme (NDOP) was developed. The NDOP is a service that allows patients to opt out of their confidential patient information being used for research and planning.

# Purpose

The purpose of this policy is to provide a consistent and logical framework to ensure that the patient's opt-out choice is respected by NHS Humber & North Yorkshire Integrated Care Board (H&NY ICB).

All health and adult social care organisations are required to be compliant with the national data opt-out policy, where they are using confidential patient information for purposes beyond an individual’s care and treatment. The Information Standard DCB3058 provides a set of requirements to ensure that all health and adult social care organisations in England can comply with the National Opt-Out.

Organisations must have a technical solution and a process in place to honour patient opt-outs. If an organisation has no uses or disclosures which need to have national data opt-outs applied, they must still put procedures in place to assess future uses or disclosures against the national data opt-out operational policy guidance.

# Definition/ Explanation of Terms

**Common Law duty of confidentiality** – In Common Law there is a duty of confidentiality which means that when a patient or service users shares information in confidence it must not be disclosed without a legal authority or justification. In practice this usually means the information cannot be disclosed without that person’s consent. (Please note Common Law consent is the consent to share information it is not the same as [GDPR consent](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/) which is a legal basis for processing personal data). GDPR Consent should not be used as the legal basis for processing data in the Public Sector. Public authorities, employers and other organisations in a position of power over individuals should avoid relying on GDPR consent unless they are confident they can demonstrate it is freely given.

**Data Controller** – A data controller determines the purposes and means of the processing, i.e., the *why* and *how* of the processing. The controller must decide on both purposes and means. Controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.

**Data Protection Impact Assessments** - A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. The ICB requires that DPIAs are considered and where necessary completed in full for any new data processing activities, new systems, services, and commissioning activities. The Information Governance (IG) Team will review and approve DPIAs and advise of requirements and recommended actions as necessary.

**Information Asset Register –** The Information Asset Register is a register of personal and business critical information held by the ICB. It details the type of information held, purpose, legal basis, location, sharing arrangements, associated risks and other detailed information.

**Message Exchange for Social Care & Health (MESH)** –NHS England’s secure messaging service. It supports the two-way transfer of data between NHS England and health and care organisations.

**NHS Spine** - NHS Digital develops and maintains the NHS Spine. The Spine allows information to be shared securely through national services such as the [Electronic Prescription Service](https://digital.nhs.uk/services/electronic-prescription-service), the [Personal Demographics Service](https://digital.nhs.uk/services/demographics), the [Summary Care Record](https://digital.nhs.uk/services/summary-care-records-scr) and the [e-Referral Service](https://digital.nhs.uk/services/e-referral-service).

**Section 251** - Section 251of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002 allows the Secretary of State for Health to make regulations to set aside the common law duty of confidence for defined medical purposes. In practice, this means the person responsible for the information can disclose confidential patient information without consent to an applicant without being in breach of the common law duty of confidence, if the requirements of the regulations are met.

# Scope of the Policy

The policy applies to NHS Humber and North Yorkshire ICB and all its employees and must be followed by all those who work for the organisation, including the Integrated Care Board, Integrated Care Partnership, those on temporary or honorary contracts, secondments, pool staff, contractors, and students.

Noncompliance with this Policy may result in disciplinary action.

# Duties/ Accountabilities and Responsibilities

## Duties within the organisation:

## Chief Executive

This is the person with overall accountability/ responsibility for this policy and will work with the Executive team to ensure compliance with legislation.

5.3 Senior information risk owner (SIRO)

Executive board member with lead responsibility for the organisation’s information risks, including any risks to ICB compliance with the National Data Opt-Out policy. They will ensure that all information risks are assessed and mitigated to an acceptable level and provide the accountable officer with assurance that information risk is managed across the ICB.

5.4 Caldicott Guardian

Executive board member responsible for protecting the confidentiality of people’s information and ensuring adherence to this policy. Ensure that procedures are in place to govern access to and the use of personal identifiable and confidential information. Provide leadership and informed guidance on complex matters involving confidentiality and information sharing.

5.5 **Senior Information Governance Manager**

The Senior Information Governance Manager is responsible for ensuring effective management, accountability, compliance, and assurance for all aspects of information governance within the organisation. The Information Governance Team will provide advice, guidance and support to all staff on any matters relating to this policy.

5.6 Information governance steering group**:** Infrastructure, implementation, monitoring and review of this document.

5.7 Line Managers **-** Line managers are responsible for ensuring that all staff particularly new staff, temporary staff, contractors, and volunteers, know what is expected of them should they be involved with processing confidential patient information for research or planning.

5.8 All staff:Supporting and adhering to this policy, in particular:

* To seek advice from the Information Governance team on whether the National Data Opt-out applies to their data activities and how it can be implemented in their area.
* Every member of staff is responsible for taking precautions to ensure the security of information, both whilst it is in their possession and when it is being transferred from one person or organisation to another. If staff are unsure about sharing information, they should refer to Information Governance Policies or take advice from their line manager, the Information Governance Team or the Caldicott Guardian, as appropriate.
* Keep up to date with best practice confidentiality and data protection procedures and legislation through undertaking annual Information Governance training.
* Understand and adhere to, Privacy and Data Protection Legislation and other legal requirements including the Confidentiality NHS Code of Practice.

## Responsibilities for approval

The Board are responsible for approving this policy.

# Policy Document Requirements

**Data Disclosures to which the National Data Opt-Out applies:**

The National Data Opt-Out applies in only limited circumstances. Broadly it applies to confidential patient information at the point it is disclosed for purposes beyond individual care which rely on Section 251 authorisation under the NHS Act 2006.

Section 251s enable the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be disclosed without the data controller being in breach of the common law duty of confidentiality. In practice, this means that the organisation responsible for the information (the data controller) can, if they wish, disclose the information to the data applicant, for example a research body, without being in breach of the common law duty of confidentiality. **To be clear - it is only in these cases where opt-outs apply.** It does not apply to data that patients have explicitly consented to share, nor to aggregated or anonymised data, only to the use of confidential data without consent.

In the NHS, the use of confidential patient information without consent is already strictly controlled. Any processing and sharing must always be in accordance with the principles of data protection legislation and the common law duty of confidentiality. Hence confidential patient information tends to be used only were essential and unavoidable. As such, many of these uses override the National Data Opt-Out.

In certain cases, it has been agreed that the NDOO should not apply to programmes which have a section 251 approval such as Invoice Validation for Controlled Environment for Finance, Assuring Transformation, and a number of National Audit Programmes. A full list of programmes with a Section 251 approval that are exempt from the NDOO can be found at: [Programmes to which the National Data Opt-Out should not be applied - NHS Digital](https://digital.nhs.uk/services/national-data-opt-out/programmes-to-which-the-national-data-opt-out-should-not-be-applied)

The programmes with Section 251 approval are subject to change so it is important that the list is regularly checked by all staff processing data that is in scope of the NDOO

**When to apply the National Data Opt-Out:**

The impact of the National Data Opt-Out is limited, particularly for ICBs, however,

any staff initiating or involved in projects that make use of confidential patient information without consent for non-care purposes should seek the advice of the IG Team unless they are certain that either a) Section 251 (of the NHS Act 2006) approval is not required and the National Data Opt-Out does not apply or b) Section 251 approval has been obtained and the project is specifically exempted from the National Data Out-Out as detailed in the list at the above link.

For further support and advice please contact:

Senior Information Governance Manager –[hnyicb-ery.ig@nhs.net](mailto:hnyicb-ery.ig@nhs.net)

**Identifying uses of Patient Data to which the National Data Opt-Out may apply:**

The ICB will identify any use of confidential patient information to which the opt-out applies via completion of data protection impact assessments (DPIAs) which explicitly ask project leads if the data is in scope of the NDOO. DPIAs should be completed for any new processing activity involving the use of confidential information, the implementation of any new system, service or data sharing arrangement.

**How to apply the National Data Opt-Out:**

Individuals who register for the National Data Opt-Out have a marker attached to their record on the NHS Spine. When the National Data Opt-Out is applied, the entire record or records associated with those individuals must be fully removed from the extract or dataset being used. It is not permitted to simply remove identifiers or otherwise de-identify part of the record.

Removal is achieved via the National Data Opt-Out’s technical solution. This requires a dedicated MESH (Message Exchange for Social Care and Health) account for sending lists of NHS Numbers to NHS Digital’s ‘Check for National Data Opt-Outs Service’ and receiving the ‘cleaned’ data back i.e., with the NHS Numbers of those who have opted-out removed. ICB staff must then use the cleaned set of NHS numbers to remove the records of opted-out patients from the dataset before sharing or otherwise processing it for a purpose to which the National Data Opt-Out applies.

The most up-to-date National Data Opt-Out must be applied at that point, i.e., all patients who have opted out at that particular time should have their data withheld. There is no need to apply Opt-Outs retrospectively i.e., to data that has already been processed or released, and there is no requirement for the ICB to remove an individual’s record from data it has already received as a result of their Opt-Out preference changing.

National Data Opt-Outs continue to apply until an individual proactively changes their Opt-Out preference. Opt-Outs are also maintained and applied for an individual after they have died.

A MESH account is available to enable ICB staff to send data sets to NHSD’s cleansing service, this can be accessed via the ICB Information Governance (see details on page 6 of this policy.)

# Consultation

The Information Governance Steering Group, which includes the SIRO, Caldicott Guardian and the Data Protection Officer have been engaged in the development of this policy.

# Training

Staff groups who may require training will be identified through the DPIA process and supported by the IG Team.

# Monitoring Compliance

The ICB will monitor uses of confidential patient data to ensure that any to which the National Data Out-Out is likely to apply are identified. The types of usage to which the National Data Opt-Out may apply include individual research projects, Clinical audit (national), risk stratification for commissioning.

Compliance will be monitored by the IG Team via completion and review of data protection impact assessments and review of the information asset register.

Information Asset Owners are responsible for ensuring they pay due consideration to the NDOO for any information assets they are responsible for.

# Arrangements for Review

This Policy will be reviewed every 3years or in line with legislative changes. The Information Governance Team are responsible for the review.

# Dissemination

This policy will be published on the ICB website and will therefore be available to both staff and the public. Staff will be informed of the publication and any subsequent changes or updates to the policy via the staff newsletter.

# Associated Documentation

All Information Governance Policies & Procedures.

# References

Information Standards Notice DCB3058 Amd 91/2018

Compliance with the National Data Opt-out – NHSD

NHS Act 2006

National Data Guardian for Health & Care: Review of Data Security, Consent and Opt-Outs

The National Data Guardian for Health & Care: Progress Report: January 2018 - March 2019

NHS Act 2006

Information Governance Policies and Procedures

NHSD Appendix 1: Section 251 of the National Health Service Act 2006

The Princes Alexandra Hospital NHS Trust

West Yorkshire Integrated Care Board

# Appendices

Appendix 1 - Anti-Fraud, Bribery and Corruption

# Impact Assessments

## Equality

NHS Humber and North Yorkshire ICB is committed to creating an environment where everyone is treated equitably and the potential for discrimination is identified and mitigated. It aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

It is required that a Quality and Equality Impact Assessment (QEIA) is carried out on a

new policy that is likely to impact on patients, carers, communities, or staff.

No adverse impact has been identified.

## Bribery Act 2010

Due consideration has been given to the Bribery Act 2010 in the development (or review, as appropriate) of this policy document, further details can be found in appendix 1.

## General Data Protection Regulations (GDPR)

The UK General Data Protection Regulation (GDPR)/ Data Protection Act 2018 includes the requirement to complete a Data Protection Impact Assessment for any processing that is likely to result in a high risk to individuals. Consideration should be given to any impact the policy may have on individual privacy; please consult NHS Humber and North Yorkshire ICB Data Protection Impact Assessment Policy. If you are commissioning a project or undertaking work that requires the processing of personal data, you must complete a Data Protection Impact Assessment.

The ICB is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and confidentiality guidance. More detailed information can be found in the Data Protection & Confidentiality Policy and related policies and procedures.

**Appendix 1 - Anti-Fraud, Bribery and Corruption**

The ICB has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from the Bribery Act 2010.  Under the Bribery Act 2010 there are four criminal offences:

•           Bribing or offering to bribe another person (Section 1)

•           Requesting, agreeing to receive or accepting a bribe (Section 2);

•           Bribing, or offering to bribe, a foreign public official (Section 6);

•           Failing to prevent bribery (Section 7).

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It should be noted that there need not be any actual giving and receiving for financial or other advantage to be gained, to commit an offence.

All individuals should be aware that in committing an act of bribery they may be subject to a penalty of up to 10 years imprisonment, an unlimited fine, or both.  They may also expose the organisation to a conviction punishable with an unlimited fine because the organisation may be liable where a person associated with it commits an act of bribery.

Individuals should also be aware that a breach of this Act renders them liable to disciplinary action by the ICB, whether or not the breach leads to prosecution.  Where a material breach is found to have occurred, the likely sanction will be loss of employment and pension rights.

To raise any suspicions of bribery and/or corruption please contact the Executive Director of Finance and Investment.  Staff may also contact the Local Counter Fraud Specialist (LCFS) at – Audit Yorkshire, email:  [nikki.cooper1@nhs.net](mailto:nikki.cooper1@nhs.net)  or mobile 07872 988939.

The LCFS or Executive Director of Finance and Investment should be the contact for any suspicions of fraud. The LCFS will inform the Executive Director of Finance and Investment if the suspicion seems well founded and will conduct a thorough investigation.  Concerns may also be discussed with the Executive Director of Finance and Investment or the Audit Committee Chair.

If staff prefer, they may call the NHS Counter Fraud reporting line on 0800 028 40 60 between 8am-6pm Monday-Friday or report online at [www.reportnhsfraud.nhs.uk](http://www.reportnhsfraud.nhs.uk).  This would be the suggested contact if there is a concern that the LCFS or the Executive Director of Finance and Investment themselves may be implicated in suspected fraud, bribery or corruption.