Nottinghamshire County Council

National Data Opt-Out Procedure

At a glance …

- The National Data Opt-Out allows individuals to opt out of their personal information being used or disclosed for indirect care (research and planning etc).
- It applies to indirect use or disclosure of data in adults care services (children's care services are excluded).
- Indirect care '*is activities that contribute to the overall provision of services to a population or to a group of people with a particular condition*.' It covers health and care services planning.
- The National Data Opt-Out has several exemptions. For instance, it does not apply to the use of identifiable information for direct care of an individual; where information is required as part of a mandatory data flows (e.g. provision of statistical data to NHS England - Digital, Office for National Statistics etc); as part of a legal obligation; where use or disclosure of the information is in the public interest; where the individual has consented to the use of their data; where the data is anonymised etc.
- The Council will ensure that all use or disclosure of confidential patient information for indirect care purposes will be assessed to establish whether the National Data Opt-Out applies.
- Where the Opt-Out applies the whole care record will be removed from the indirect care use, not just the personal identifiers.
- When personal health or care data is being used for purposes which fall into the scope of the Opt-Out, contact will need to be made with NHS England - Digital to establish the NHS numbers of those individuals that have not opted out.
- The Business Intelligence Unit (BIU) provides advice and support on depersonalising (anonymising / pseudonymising) personal information; applying the National Data Opt-Out and obtaining details of NHS numbers that can be used for indirect care purposes from NHS England - Digital.

Purpose

1. This document sets out Nottinghamshire County Council's procedure complying with the National Data Opt-Out.

2. It forms part of the suite of documents that comprise the Council's Information Governance Framework.

Background

3. The National Data Opt-Out allows users of adult social care and health services in England to opt out of their confidential patient information being used or disclosed for purposes beyond their direct care (sometimes termed individual care), unless a specific exemption applies.

4. The government requires organisations that provide health and adult social care services to have in place systems and processes so that they can apply people's Opt-Out choices to the indirect care use of data (e.g. research and planning etc).

5. Compliance with the National Data Opt-Out is tested in the Council's annual Data Security and Protection (DSP) Toolkit self-assessment submission. An organisation which meets Toolkit standards is considered suitable for NHS bodies to share heath data with.

6. The Opt-Out is a part of the drive to develop a digitised health and care system. This relies on individual's trusting that their data is safe, secure and their privacy is protected.

7. NHS England - Digital has issued a detailed National data opt out operational policy guidance document. This Council Procedure distils that advice and explains how the Council will apply and comply with the Opt-Out.

Definitions

8. Personal data as defined in the Data Protection Act 2018, is any information relating to a living person which may directly or indirectly identify them.

9. Confidential patient information is information that can identify an individual coupled with information about their health, care or treatment. Confidential patient information applies to living and deceased people.

10. The definition of "patient" includes an individual who needs or receives local authority social care or, whose need for such care, is being assessed by a local authority.

11. Personal or confidential patient information can be in any format including paper, electronic, digital images, voice recordings etc. Processing of information includes anything you might do with it.

12. Direct care is '*a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society*.' [Caldicott Review]

13. Indirect care '*is activities that contribute to the overall provision of services to a population or to a group of people with a particular condition*.' It covers health and care services planning (e.g. improving and enabling the efficient and safe provision of health and care services) and research (e.g. finding ways to improve treatments, identify causes of and cures for illness).

Scope

14. This Procedure applies to the processing of all Council adult's confidential patient information used for indirect care purposes from April 2022 onwards except where a valid exemption applies (see later).

15. Generally, within adults' social care, and supported services, aggregated information is, and should be, being used for planning or commissioning purposes, so that identifiable information such as personal information is not included; only sub-totals and totals are shown.

16. The Opt-Out does not apply the historic processing of Council confidential patient information used for indirect care purposes prior to July 2022.

17. The Opt-Out will not be able to be applied for a small and reducing percentage of adult social care service users whose NHS numbers are not held by the Council. There is no obligation to 'trace' NHS numbers for the purposes of the Opt-Out but, in any case, the Council is actively trying to increase NHS number coverage in its Mosaic system to enhance is ambitions of integration with health.

18. Where the Council is contracting external providers, and the use / disclosure of data would be in scope for the Opt-Out, advice should be sought, and consideration should be given to making it part of the tender process and contract to require evidence of compliance with National Data Opt-Out.

19. The National Data Opt-Out sits alongside the UK General Data Protection Regulation (UK GDPR).

Principles & Commitments

20. The Council will ensure that all use / disclosure of confidential patient information for indirect care purposes will be assessed to establish whether the National Data Opt-Out applies.

21. Where it does apply, this Procedure will be followed to ensure the agreed process is followed.

22. Where a decision not to apply the Opt-Out to the use / disclosure of patient confidential information for indirect care is taken, and the rationale for that decision is not obvious (e.g. an exemption clearly applies), a brief written note

of the reason not to apply the Opt-Out will be kept by the team that is responsible undertaking the indirect care data processing.

23. Where the Opt-Out applies, the whole care record will be removed for the indirect care use, not just the personal identifiers.

24. Appropriate reference will be made to the National Data Opt-Out in the Council's privacy notice(s).

25. The Council will maintain a published statement of compliance to support wider privacy and transparency information on the National Data Opt-Out.

The Opt-Out, UK GDPR and Confidentiality

26. The UK GDPR requires that processing of personal data is '*fair, lawful and transparent.'* To be lawful there must be valid grounds under the UK GDPR for processing the data (known as 'legal basis for processing') but also, the data must not be processed in a way which breaches any other UK law.

27. The common law duty of confidence (confidentiality) applies when one person discloses information to another (e.g. patient to care worker) in circumstances where it is reasonable to expect that the information will be held in confidence.

28. So, for the processing of patient confidential information to be lawful, the UK GDPR **and** the common law duty of confidence must be satisfied.

29. The Council has extensive statutory obligations and powers and rarely needs to use consent as the legal basis for personal data processing under the UK GDPR. However, to respect common law duty of confidence there should be consent from a patient / user of social care services for the use / disclosure of their data or, alternatively, there should be another legal basis which enables the common law duty to be set aside (i.e. a legitimate reason not to abide by it).

30. Most patients / users of social care services understand and expect that relevant information sharing enhances their care. Guidance is that relevant information can be shared with those who provide or support direct care to an individual, unless the patient has objected [see Confidentiality: good practice in handling patient information, General Medical Council (GMC), 2024, para 30].

31. The National Data Opt-Out allows for the common law duty of confidence to use confidential patient data for indirect care purposes by proactively publicising and giving people the opportunity to object (opt-out) up front, except where an exemption applies.

Exemptions to the National Data Opt-Out

32. The National Data Opt-Out will apply to all indirect uses / disclosure of patient confidential information unless:

a) The data is processed for direct care purposes (e.g. data shared between health and care professional in a hospital). Direct care also includes:
   - the management or supervision of cases
   - activity to sub-contract services
   - carrying out case audits
   - use of performance statistics and dashboards to help manage caseloads
   - use of data to support the supply and delivery of direct care
   - payment and invoice validation (though guidance is that anonymised data should be used for this purpose)
   - risk stratification for case finding (i.e. a systematic process to identify sectors of the population that may benefit from additional clinical intervention, where carried out by a provider involved in an individual's care).

b) The data relates to children's social care.

c) The data is provided to comply with requirements for mandatory data flows (e.g. provision of statistical data to NHS England, Office for National Statistics, data provided to NHS England under s259 of the Health and Social Care Act (HSCA) 2012 etc).

d) The data is processed to meet a legal obligation, that is information required by law or a court order. This may include providing CQC with information for their statutory inspections; coroners investigations; reports to the Health and Safety Executive; sharing information for safeguarding purposes etc.

e) The individual has explicitly consented to their data being used for indirect care purposes (e.g. where they may have opted out at the national level but agreed to participate in a local research project etc). In these situations, individual consents need to be recorded and retained.

f) The data is for disclosure in relation to the monitoring and control of communicable disease and other risks to public health.

g) There is an overriding public interest to process the data (e.g. in an emergency or in a situation when the safety of others is most important when the public interest in disclosing the data overrides maintaining confidentiality).

h) The data is rendered unidentifiable (anonymised) or is aggregated or count data in line with the ICO Anonymisation: managing data protection risk code of practice.

The Opt-Out Process

For the individual

33. Individuals (or someone acting as their proxy) register their decision to opt out with the NHS via the following web link https://www.nhs.uk/your-nhs-data-matters/ or by post or phone. If an individual contacts the Council asking to opt out, then they should be signposted to these details.

34. Where an individual has a complaint or query about how the Council applied or not applied their opt out choice, they should be referred the Data Protection Officer (DPO@nottscc.gov.uk). Alternatively, queries can be addressed to the Information Governance Team (data.protection@nottscc.gov.uk).

For the Council

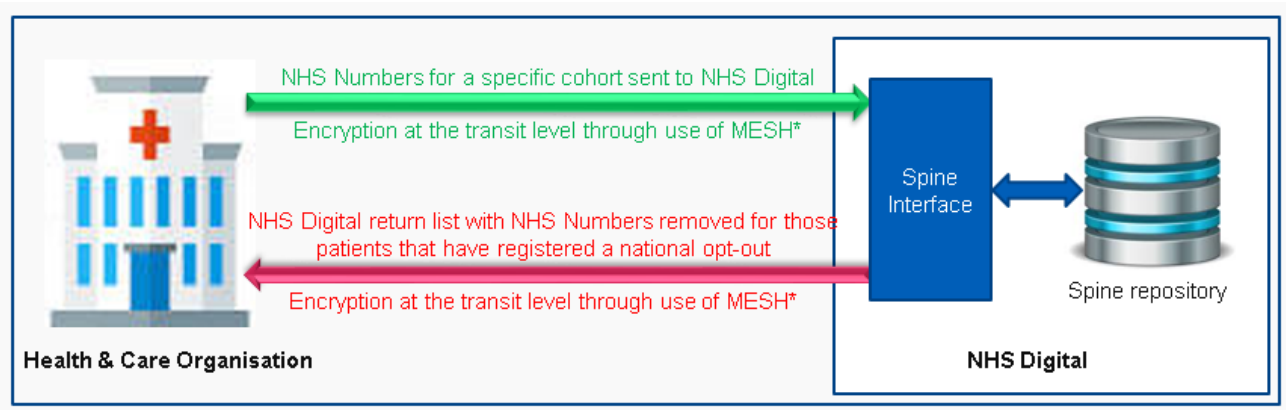
35. The decision to opt out is then recorded against their NHS number and stored by NHS England - Digital. The individual's opt out choice remains in place during their life time unless they change their mind. Opt outs remain in place after a person has died.

36. When the Council intends use or disclose data for indirect care purposes, it will first need to remove the whole record of any individual who has opted out, unless a legitimate exemption applies. Changed or new processing of personal data triggers the Data Protection Impact Assessment (DPIA) process and a summary DPIA will need to be completed.

37. The Business Intelligence Unit (BIU) provides support to Council services in applying the Opt-Out. It will advise on when the Opt-Out applies (seeking advice from the Information Governance Team where needed); assist in identifying the data to be processed; and seek confirmation of the data that can be used. The steps that will be taken are set out below.

38. The first step is to identify and create a full list of individuals whose data is to be used / disclosed. Those individuals' NHS numbers will then need to be checked to identify those that have not registered an opt-out.

39. The list of NHS numbers is submitted to check for opt outs via the secure Message Exchange for Social Care and Health (MESH) messaging service, an external service provided by NHS England - Digital. The service checks the list of NHS numbers against a list of opt-outs collected by the NHS (in the NHS Spine). Where a match is found, the individual's NHS number is removed and an updated list of NHS numbers (with opt-outs removed) is returned to the Council via the MESH. The following diagram illustrates the process:



40. This then becomes the list of individuals whose data can be used for indirect care purposes.

41. In order to make for an efficient and proportionate process to comply with the Opt-Out, the BIU will seek confirmation of eligible NHS numbers on a monthly basis, although the frequency of this will be kept under review.

42. Where data is being shared which has had the Opt-Out applied, the recipient of the data should be made aware of that. The Council's Information Sharing Agreement template will include provision for the application of the Opt-Out to be referenced.

Roles and Responsibilities

43. All Council staff with who are accountable or responsible for using patient confidential information for indirect care purposes (research and planning) must comply with this Procedure.

44. The Caldicott Guardian is accountable for ensuring that the Council applies the National Data Opt-Out.

45. The Council's Data Protection Officer and Information Governance Team will support the Caldicott Guardian to ensure that the requirements described in this procedure are implemented and maintained and will handle any queries or complaints from individuals about the Council's application of the Opt-Out.

46. The Business Intelligence Unit (BIU) will provide advice and guidance on applying the Opt-Out and will have the technology to contact the NHS (MESH) messaging service to establish the opt out status of particular cohorts of NHS numbers (on a routine or one-off basis).

47. ICT will ensure that the technology is in place to enable the Council to securely send and receive NHS numbers to and from the NHS MESH.

48. Duties assigned to specific roles referenced in this procedure must be carried out as described. The Council's Information Governance Framework provides

further detail of the nature of specific information governance related roles (e.g. that of SIRO, Caldicott Guardian, Data Protection Officer, Information Asset Owner, Information Asset Manager etc.) see also the intranet page on IG roles and responsibilities.

Compliance with this Procedure

49. Wilful or negligent disregard for information governance policies and procedures will be investigated and may be treated as a disciplinary matter under the relevant employment procedure(s) which could lead to dismissal or the termination of work agreements or service contracts.

Review of this procedure

50. This procedure will be regularly monitored and reviewed by the Data Protection Officer (or their nominee) who will revise it in line with learning arising from its implementation.

51. Beyond that, the procedure will be monitored and reviewed every two years in line with legislation and codes of good practice.

Advice, Support & Further Information

52. For advice on depersonalising (anonymising / pseudonymising) personal information; applying the National Data Opt-Out or to obtain details of NHS numbers that can be used for indirect care purposes, please contact:

    The Business Intelligence Unit
    Email: policy@nottscc.gov.uk

53. If you have any issues over the clarity of this procedure, or want further advice on the National Data Opt-Out, please contact:

    The Information Governance Team
    Email: data.protection@nottscc.gov.uk
    Telephone: 0115 8043800

54. Further reading and supporting information:

Title (as hypertext link) and publication date	Author
National data opt out operational guidance document	NHS England - Digital

Document Control

Owner	Data Protection Officer
Author	Caroline Agnew

Last Reviewer	Megan Bilton
Approver	Information Governance Board
Date of Approval	06/03/2020
Date of next review	23/10/2028
Version	1.2
Classification	Public

Version	Date	Changes and Approver
1.0	06/03/2020	Information Governance Board
1.1	14/03/2022	Minor updates by Information Governance Team
1.2	23/10/2025	Review by Information Governance Team with no major amends