

The national data opt-out allows a patient to choose whether or not they will allow their confidential patient information to be used for purposes beyond their individual care and treatment. For example, for research or business planning. The Policy allows service users, or the persons acting for them by proxy, control over setting or changing their own opt-out choice. They may change their mind at any time.

These preferences must be recorded on the national system by completing a form on the NHS Your Data Matters website, on the Your Data Matters app, or by phone. GPs may also be notified in line with a service agreement to update these preferences on behalf of a provider. Preferences are then recorded against the person's NHS number on the Spine (a national NHS database).

Compliance with this Policy is mandatory for all health and social care organisations and a requirement of the NHS Data Security Protection Toolkit.

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. Such purposes include, but are not limited to:

- **Planning**

Such as predicting what services will be needed in the future, so funding and resources can be put into place or reviewing patient records to understand outcomes of patient care.

Sometimes health and care services work in partnership with commercial organisations to plan and provide services. For example, health and care analysis companies can be employed by NHS trusts and care organisations to measure effectiveness and identify improvements. The NHS organisation and local authority providing the data have all legal responsibility for it and puts a contract in place to cover the data sharing arrangements.

- **Research**

Such as reviewing multiple service user records or data sets to research diseases and illnesses and their treatments to see whether there are side effects or risk factors associated with certain medications, identifying risk factors for disease and its severity, or monitoring the effects of a new drug or type of treatment.

The Policy does not apply where consent has been gained for the activity, the purpose is necessary for compliance with a legal obligation or to fulfil a contract to which the data subject is party or the data is anonymised in line with the ICO's Code of Practice on Anonymisation. It does

not apply to children's social care services or services outside of England. It may be overridden by a Public Interest Test which determines that disclosure or use is in the substantial public interest, for example reviewing records for the purposes of preventing a public outbreak of disease.

The opt-out applies regardless of the format of the data and this includes structured and unstructured electronic data and paper records. When the opt-out is applied, the entire record (or records) associated with that individual must be fully removed from the data being disclosed. The NHS number is normally used as the identifier for the removal of the records.

Which data disclosures do national data opt-outs apply to?

National data opt-outs apply to a disclosure when an organisation, for example a health research or planning body, confirms they have approval from the Confidentiality Advisory Group (CAG) for the disclosure of confidential patient information held by the local authority who is responsible for the data (the data controller).

The CAG approval is also known as a section 251 approval and refers to section 251 of the National Health Service Act 2006 and its current Regulations, the Health Service (Control of Patient Information) Regulations 2002. The NHS Act 2006 and the Regulations 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 local authority can disclose information to the data 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.**

Nottingham City Council has not recorded any such approaches from research or health planning related organisations in recent years. However, when such an approach is received, the Council will handle it in line with the [National data-opt-out operational-policy guidance](#) produced by NHS Digital and in accordance with its own information rights policies and procedures as set out at <https://www.nottinghamcity.gov.uk/privacy-statement> .

The Data Controller is Nottingham City Council, Loxley House, Station Street, Nottingham, NG2 3NG.

The Data Protection Officer is Naomi Matthews. You can contact the data protection officer at the above address or at data.protectionofficer@nottinghamcity.gov.uk .

The data protection law known as the General Data Protection Regulation provides for the following rights as prescribed by the legislation:

- A right to request a copy of your information
- A right to request rectification of inaccurate personal data
- A right to request erasure of your data known as 'the right to be forgotten'
- A right to in certain circumstances to request restriction of processing
- A right in certain circumstances to request portability of your data to another provider
- A right to object to processing of data in certain circumstances

- A right regarding automated decision making including profiling

Please note that if you are unhappy with a decision regarding the handling of your data you have the right to complain to the Information Commissioner's Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. See also the Information Commissioners website at <https://ico.org.uk/your-data-matters/> .

For more information about these rights please refer to our detailed privacy statement at <https://www.nottinghamcity.gov.uk/privacy-statement> .