National Data Opt-out: Factsheet 4 – How it is applied

This is one of a series of factsheets about data uses and the national data opt-out

Published 25 May 2018

Factsheet 4 – How it is applied

Purpose

This factsheet provides information for health and care organisations about their responsibilities and the rules when applying national data opt-outs.

This is an overview only and more detail is provided in the National Data Opt-out Operational Policy guidance document published at: https://digital.nhs.uk/national-data-opt-out.

The national data opt-out (offered to the public as '*Your Data Matters to the NHS*')

The national data opt-out allows a patient to choose that they do not want their **confidential patient information** to be used for purposes beyond their individual care and treatment.

Information is detailed below about the responsibilities of organisations to consider the national data opt-out and how to apply it.

Details of organisations and types of record that the national data opt-out applies to can be found in Factsheet 3 - "What data and organisations it applies to".

Responsibilities for applying the national data opt-out

All health and care organisations that act as a sole data controller or a joint data controller for patient data have a responsibility to consider the national data opt-out policy and ensure it is being applied in accordance with the policy and in line with the wider implementation timetable.

A data controller is a person acting on behalf of an organisation who (either alone or jointly with other persons) determines the purposes for which and the way any data is or is to be processed. For more information on data controllers see: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

Data controllers must also ensure that any other organisation acting as a data processor on their behalf is also applying the national data opt-out, in accordance with the policy.

In general, where section 251 is being relied upon as the lawful basis (under the Common Law Duty of Confidentiality) to process confidential patient information then the national data opt-out will apply. In exceptional circumstances the Confidentiality Advisory Group (CAG), which provides independent expert advice on section 251 applications, may recommend that the national data opt-out does not need to be applied. The data controller will need to satisfy themselves that such an exemption has been given, for example, they could request sight of the CAG approval letter which should clearly indicate that national data opt-outs do not apply, before they provide any data.

Factsheet 2 – "When it applies" contains further information about the data uses when the national data opt-out does and does not apply.

Factsheet 1B – "Types of data used and legal protection in place" contains further information about section 251 approvals.

Timescales for applying national data opt-outs

From 25 May 2018, when the national data opt-out service is introduced, NHS Digital will apply national data opt-outs in line with the policy. It can take up to 21 days from the time the opt-out is first registered before it can take effect to remove a patient record from data being provided to another organisation.

It will take time to be able to implement the technical solution and operational processes required for all health and care organisations to be able to apply the national data opt-out. Further information about the

implementation approach for other organisations to apply the opt-out can be found at: https://digital.nhs.uk/national-data-opt-out.

The implementation timescales were set out by the Government in their response to the National Data Guardian (NDG) review, see: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf.

Application of the national data opt-out

NHS Digital has developed the service and systems to enable patients to set, view and change their national data opt-out choice. National data opt-outs are stored centrally in a separate opt-out repository on the NHS Spine, against the patients' NHS numbers. NHS Digital are the data controller for patients' national opt-out data and have responsibility for ensuring that all national data opt-outs recorded by patients, and any changes to a patient's national data opt-out, are processed accurately and recorded in the opt-out repository on the NHS Spine.

Individual health and care organisations must not maintain local lists of patients who have a national data opt-out.

The NHS number is the sole identifier used to apply national data opt-outs.

A technical solution will be provided by NHS Digital to access the NHS Spine opt-out repository to enable NHS numbers to be matched to the list of national data opt-outs for the purposes of applying national data opt-outs. Separate guidance on the technical solution will be available at: https://digital.nhs.uk/national-data-opt-out.

The national data opt-out must be applied where an NHS number is or was available as part of the data that the organisation holds, including where the organisation can easily locate the NHS number, for example where they have other data for the patient that already includes it. Outside of existing good practice processes for improving data quality and tracing patients to identify their NHS number, organisations are not expected to specifically trace missing NHS numbers in any data or records where national data opt-outs are to be applied.

Organisations must not deliberately remove NHS numbers from a set of data or records to prevent national data opt-outs from being applied, other than in cases where there is a legal requirement to remove such identifiers from the record. In these cases, such as records about In Vitro Fertilisation (IVF) which are restricted under the Human Fertilisation and Embryology (HFE) Act 1990 and HFE (Disclosure of Information) Act 1992, there must be no attempt to re-identify the records so that national data opt-outs can be applied.

An organisation must remove the entire record (or records) for the patient from the data that is going to be disclosed for a specific purpose where there is a match on the NHS number and the national data opt-out policy applies. It is not sufficient to remove identifiers or to otherwise anonymise that patient's data. This is in the spirit of the offer that has been made to patients – that their confidential patient information will not be used for those purposes. The removal of identifiers in this way does not render the data as anonymised, in line with the Information Commissioner's Office (ICO) code of practice on anonymisation. Re-identification may still be possible from any combination of data items that the organisation receiving the data may hold. To manage this risk either the full record is removed for those with opt-outs or the entirety of the data being supplied should be provided in an anonymised form that is compliant with the ICO code of practice, including the technical and organisational controls as required by the code.

There may be limited scenarios where a record contains information about more than one patient, such as a maternity record that may hold some details about both the mother and baby or babies. In this event, organisations should make best efforts to apply the national data opt-out for each individual in the record (subject to NHS numbers being available for each patient), and to remove the whole record. So, in the example of a record about patient X that also contains information about patient Y and patient Z, if any one of those patients has a national data opt-out, patient X's record should be identified and removed.

Different formats of data

The national data opt-out applies to both electronic information, such as a file produced from a database or from a spreadsheet, and non-electronic forms of information such as paper records.

The national data opt-out applies to both structured and unstructured data. Structured data is data that is set out in an organised standard way and is easily searchable such as a list of patients and information about them set out in a regular pattern of fields in a spreadsheet or a table within a document. Unstructured data does not follow a standard format or layout and could be information in the form of notes or a letter.

How long does a patient's national data opt-out last?

Once a national data opt-out is set, it remains in place until a patient changes their mind. A patient can change their national data opt-out choice at any time.

Further information about setting or changing a national data opt-out can be found in Factsheet 5 – "Setting a national data opt-out".

Does the national data opt-out need to be applied retrospectively?

The national data opt-out does not apply retrospectively so, for instance, data provided to another organisation before an opt-out was set by a patient should not be recalled to have the national data opt-out applied and then be reissued.

What happens if a patient does not live in England?

Where a patient has set a national data opt-out it must be applied in line with the policy regardless of whether the patient currently resides in England or has ever resided in England. Patients can set an opt-out if their details are registered on the Personal Demographics Service and they have an NHS number, and this is not reliant on them being resident in England.

What happens when a patient dies?

Where a patient has set an opt-out and then dies their national data opt-out must continue to be applied, in line with the policy.

Keeping records of data uses and application of the national data opt-out

Health and care organisations should maintain records of data processing activities, including the legal basis for that processing. These records should also document whether the national data opt-out has been applied.

All organisations with access to NHS patient data and systems must use and complete the national Data Security and Protection (DSP) Toolkit to provide assurance that they are complying with the 10 data security standards as set out in the National Data Guardian "Review of Data Security, Consent and Opt-Outs". The national data opt-out is included in the DSP toolkit and organisations are required to provide evidence of the lawful basis for any data processing activity and whether national data opt-outs have been applied. This appears under Data Security Standard 1, Assertion 1.4 within the DSP Toolkit. See https://www.dsptoolkit.nhs.uk/.

Other opt-outs

Where a patient has a national data opt-out in place alongside any other form of opt-out(s) the other opt-out(s) must still be applied in accordance with the policy for each specific opt-out.

Further information about other opt-outs can be found in Factsheet 5 – "Setting a national data opt-out".