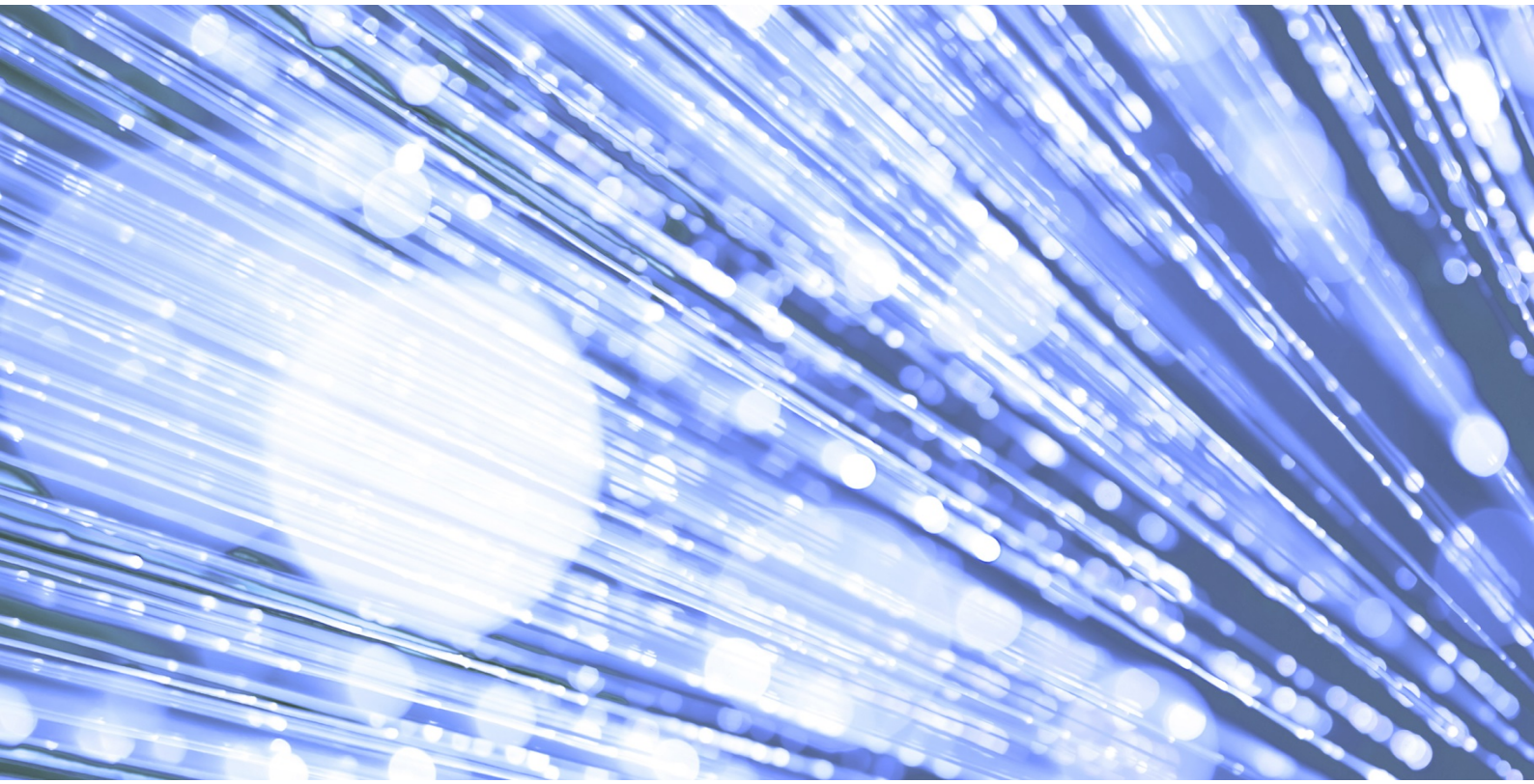
DCB3058 Compliance with National Data Opt-outs

Requirements Specification

Published 18 March 2019



Information and technology
for better health and care

Data Coordination Board

This information standard (DCB3058) has been approved for publication by the Department of Health and Social Care under section 250 of the Health and Social Care Act 2012.

Assurance that this information standard meets the requirements of the Act and is appropriate for the use specified in the specification document has been provided by the Data Coordination Board (DCB), a sub-group of the Digital Delivery Board.

This information standard comprises the following documents:

- Requirements Specification
- Implementation Guidance.

An Information Standards Notice (DCB3058 Amd 91/2018) has been issued as a notification of use and implementation timescales. Please read this alongside the documents for the standard.

The controlled versions of these documents can be found on the NHS Digital website. Any copies held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Date of publication: 18 March 2019

Glossary of Terms

Term / Abbreviation	What it stands for
CPI	Confidential Patient Information
DHSC	Department of Health and Social Care
DPIA	Data Protection Impact Assessment
DSP	Data Security and Protection
GDPR	General Data Protection Regulation
GP	General Practitioner
ICO	Information Commissioner's Office
ICT	Information and Communications Technology
NDG	National Data Guardian
NHS	National Health Service
UK	United Kingdom

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1. Introduction

This standard is in response to the National Data Guardian (NDG) Review of Data Security, Consent and Opt-outs (see Ref 2 weblink in the supporting documentation table below) and the Government Response – Your Data: Better Security, Better Choice, Better Care (see Ref 3 weblink in the supporting documentation table below), and is designed to provide a set of requirements to enable health and adult social care organisations to be compliant with the national data opt-out.

It mandates organisations to be compliant with the national data opt-out operational policy in accordance with this 'DCB3058 Compliance with National Data Opt-outs' standard, which includes the National Data Opt-out Requirements Specification and Implementation Guidance (based on the National Data Opt-out Operational Policy Guidance, the National Data Opt-out Compliance Implementation Guidance, and the National Data Opt-out Technical Guidance made available via NHS Digital).

1.1 Purpose

The purpose of this document is to set out the requirements to enable Health and Adult Social Care organisations that are in scope of this standard to comply with national data opt-outs.

It is accompanied with implementation guidance describing how organisations can meet the requirements.

1.2 Supporting Documents

This information standard is supported by the following documentation:

Ref	Reference	Title	Purpose
1	NHS Digital Website / National Data Opt-Out	National Data Opt-out Operational Policy Guidance	This document sets out the policy rules for all health and adult social care organisations to use when assessing whether the national data opt-out needs to be applied.
2	UK Gov website	National Data Guardian for Health and Care – Review of Data Security, Consent and Opt-outs	This document sets out recommendations to strengthen security of health and care information and ensure people can make informed choices about how their data is used.
3	UK Gov Website	Government Response – Your Data: Better Security, Better Choice, Better Care	This document sets out the Government's Response to the National Data Guardian's Review on Data Security, Consent and Opt-Outs, and the Care Quality Commission's Review 'Safe

			Data, Safe Care'. It provides a summary of consultation responses and sets out the Government's proposed approach.
4	NHS Digital Website / Directions	Direction issued to NHS Digital on 12September 2017, and 21May 2018	These two Directions were given by the Secretary of State for Health and Social Care requiring NHS Digital to establish and operate a system for the collection and analysis of information, and to exercise such systems delivering functions, in respect of the national data opt-out model.

1.3 Legal, strategic and policy context

The national data opt-out is a Department of Health and Social Care (DHSC) policy that provides choice to patients about how their confidential patient information is used for purposes other than their individual care and treatment.

The NHS Constitution pledges that where a patient's identifiable information must be used:

- patients are given the chance to object wherever possible, and that
- patients have the right to request that their confidential information is not used beyond their own care and treatment and
- to have objections considered, and where patients' wishes cannot be followed, to be told the reasons including legal basis

However, the NHS Constitution does not provide an absolute right to stop confidential information flowing, for example, the use of personal data to prevent the spread of infection of notifiable diseases and to prevent further outbreaks in future.

The National Data Guardian's "Review of Data Security, Consent and Opt-outs", accepted by the Government in their response "Your Data: Better Security, Better Choice, Better Care", recognised there was no easy way for patients to object and recommended the implementation of the national data opt-out across health and care services within England.

The national data opt-out is a policy offer in addition to the legal rights of data subjects provided via data protection legislation. The implementation of the national data opt-out does not change or remove any legal obligations on any organisation including the Data Protection Act 2018 and General Data Protection Regulation (GDPR). For the avoidance of doubt, health and adult social care organisations must separately make provision for patients to exercise their legal right to object and the national data opt-out does not change or remove this requirement. Further information on how this affects compliance

and the application of the national data opt-out is set out in section 2.4 of the National Data Opt-out Operational Policy Guidance.

Under Direction from the Department of Health and Social Care (DHSC), NHS Digital have been instructed to provide a national data opt-out service that can be used by all in scope health and care organisations under two separate Directions:

1. On 12 September 2017, the Department of Health and Social Care issued a Direction to NHS Digital to:

(1) Collect the 'patient opt-out data', namely the record of those individuals who have registered an opt-out and store these against an individual's NHS number, as well as relevant technical (or meta) data related to the setting of that opt-out e.g. time and date etc. for audit purposes.

(2) Establish a national repository for central storage of the patient opt-out data.

(3) Establish a new national opt-out system to enable health and care organisations to access the patient opt-outs data from the national repository, for the purposes of applying patient opt-outs to the patient data that they disseminate in accordance with the opt-out policy.

This direction provides the legal basis for NHS Digital to collect NHS numbers i.e. the flow of lists of NHS numbers into and out of NHS Digital.

The direction further requires NHS Digital to provide a national repository for the central storage of the patient opt-out data and "a new national opt-out system to enable health and care organisations to access the patient opt-out data from the national repository". A service to check for and remove NHS numbers of those patients that have a national data opt-out has been developed by NHS Digital to deliver this, in that it provides the necessary information back to health and care organisations to enable them to uphold national data opt-outs for their disclosures of confidential patient information.

(2) On 21 May 2018 the Department of Health and Social Care issued a 2nd Direction instructing NHS Digital:

With effect from 25 May 2018, NHS Digital is directed to start to operate the system to process and to commence upholding of the national data opt-out. National data opt-outs will apply to the use of confidential patient information for purposes beyond direct care, in accordance with the published policy. NHS Digital is directed to publish and maintain this policy guidance which will be set by DHSC ministers and policy officials. All organisations providing health services or adult social care in England, or otherwise exercising functions relating to health or adult social care, will be responsible for upholding the national data opt-out in accordance with the latest policy guidance and in line with the timetable set by DHSC for the implementation phase.

This direction provides the legal basis for NHS Digital to provide the service to check for and remove NHS numbers of those patients that have a national data opt-out to enable health and care organisations to apply national data opt-outs as required.

NHS Digital's National Data Opt-out Programme has developed and delivered a public facing service which enables patients to set a national data opt-out preference. The service provides information to enable patients to make an informed decision and can be accessed through a range of channels including online. In addition, NHS Digital has developed a range of guidance and materials that support all health and adult social care organisations to become compliant with the national data opt-out policy, including the provision of a service to check for national data opt-outs.

1.4 Scope

This standard sets out the obligations to health and social care organisations to comply with these requirements (see section 2 below). It mandates and supports all health and adult social care organisations to operate systems and processes to be able to be compliant with the national data opt-out. For further information about being compliant with the national data opt-out, please refer to the 'Compliancy Implementation Guide' document.

This standard applies to organisations that handle data that originates within the health and adult social care system in England and includes:

- Department of Health and Social Care and other national bodies e.g. NHS England
- NHS bodies and Local Authorities providing health and adult social care services in England; and
- other organisations or persons who provide health or adult social care services in England under contracts agreed with NHS and Local Authorities.

The scope of health and adult social care organisations set out above is in line with the Health and Social Care Act 2012 section 250 definition of organisations required to have regard to published information standards.

The National Data Opt-out Operational Policy Guidance provides further information on the organisations that are included and excluded from this definition.

Broadly it includes (but is not limited to) health service providers (e.g. NHS Trusts, GP practices), private providers who deliver services which are publicly funded, commissioners of health and care services (e.g. Clinical Commissioning Groups and Local Authorities) and Arms-Length Bodies.

An organisation can be in scope but may not have **any** data disclosures which require the actual application of national data opt-outs, for example:

- because the data being disclosed is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice on Anonymisation, or
- consent has been obtained from the individual for their data to be used for the specific purpose, or
- the organisation only uses Confidential Patient Information (CPI) for individual care, or
- because the data is being provided under a mandatory legal requirement or is deemed to be in the public interest.

In such cases an organisation must still be compliant with the national data opt-out standard even though they do not need to apply national data opt-outs. However, all organisations in scope must have processes and procedures in place to ensure that they remain compliant should any changes occur that may require them to apply national data opt-outs to existing or future data disclosures.

This standard applies to private providers only **where the treatment or care is being coordinated, funded or commissioned by a public body** such as a local authority.

1.5 Out of scope

This standard does not apply to organisations and services that are not part of the health and adult social care system in England as national data opt-outs do not apply to organisations and services which are not part of the health and adult social care system in England. For example:

- providers of Children's services (including children's social care, education services and schools) which are regulated by Ofsted or otherwise within the policy responsibility of Department for Education (DfE) (N.B. child health services provided through organisations regulated by CQC do remain in scope)
- 'health' related data which originates and is shared by organisations completely outside of the health and adult social care system in England
- private providers where a patient is privately funding their individual care and treatment.

2. Compliance with National Data Opt-out Requirements

2.1 Requirements definition

The requirements within this specification are assigned levels using the IETF RFC2119 convention, namely:

MUST - This word, or the term "SHALL", mean that the definition is an absolute requirement of the specification.

SHOULD - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

MAY - This word, or the adjective "OPTIONAL", mean that an item is truly optional. One organisation may choose to include the item because a particular marketplace requires it or because the organisation feels that it enhances the product while another organisation may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

2.2 Requirements

Reference	Requirement
1	The national data opt-out **MUST** be respected and applied if appropriate by health and adult social care organisations in England[1].
2	Implementation guidance supporting the standard **MUST** be considered to ensure compliance with national data opt-out policy. Organisations SHOULD read all relevant documentation but **MUST** read and adhere to the National Data Opt-out Operational Policy Guidance; Compliancy Implementation Guide; and if required to apply opt-outs the User Guidance (MESH Guidance for using the Check for National Data Opt-outs Service).
3	Organisations **MUST** make sure any patients wishing to opt-out of the use of their confidential patient information for purposes beyond individual care are informed about the national data opt-out and signposted to the relevant information.
4	Organisations **MUST** make sure relevant staff are informed and trained about the national data opt-out and are able to appropriately support and signpost patients wishing to opt-out of the use of their confidential patient information for purposes beyond individual care.
5	Organisations handling confidential patient information **MUST** have in place appropriate procedures so that on an ongoing basis they can: • identify any data disclosures where national data opt-outs need to be applied in line with the National Data Opt-out Operational Policy Guidance (it should be noted that procedures **MUST** be effective for pre-existing and any new data disclosures). • apply the national data opt-out in line with the published information standard for compliance with the national data opt-out.
6	Organisations **MUST** inform patients of their compliance with the national data opt-out policy and the standard in line with the agreed timelines for implementation.
7	Organisations applying the national data opt-out **MAY** provide information to the data recipient on the number of records removed due to the application of national data opt-outs.

[1] National data opt-out was launched in May 2018 and will be fully implemented by March 2020. More information is available on the national data opt-out programme webpages.

2.3 Conformance Criteria

The following specific conformance criteria will be used post implementation to demonstrate conformance:

1	**Data Security and Protection (DSP)Toolkit** Organisations operating via the NHS Standard Contract **MUST** have completed the DSP Toolkit and published their annual submission on time.
2	**Data assessment** Organisations **MUST** have provided evidence that they have assessed their data uses against the national data opt-out policy.
3	**Applying National Data Opt-out processes** Organisations **MUST** have processes in place that enable them to apply the national data opt-out where needed. This **MAY** include details of how and when the national data opt-out has been applied to specific disclosures of confidential patient information processed within their organisation through a data release register or other transparency materials.
4	**Statement of compliance** All other health and adult social care organisations that do not operate via the NHS Standard Contract **MUST** have published a statement of compliance that is available to the public. This **MAY** be published on their website or in a privacy notice. This weblink details information to support the development of a privacy notice.
5	**Informing patients** Organisations **MUST** have evidence that shows how and when they have informed patients about the national data opt-out. A range of accessible public communication materials have been developed by NHS Digital and organisations **MAY** make these available to their patients.
6	**Staff training and competency** Staff and professionals involved in the disclosure of data **MUST** have received appropriate and timely training to enable effective implementation of this standard when their organisation is required to be compliant with national data opt-outs. Organisations **MUST** have evidence of training which **SHOULD** be: • training records that indicate that relevant staff and professionals have received any training identified as locally necessary to enable effective implementation of the standard. • evidence that the national data opt-out is included in staff guidance on confidentiality and data protection issues, and that this guidance documentation has been approved via local governance processes.

7	**Organisational processes and controls** Organisations **MUST** have processes and controls in place for effective implementation of the standard. For example; where data disclosures have been assessed to require the application of the national data opt-out the organisation **MUST** have accessed the service to check for national data opt-outs to submit and receive NHS numbers enabling the removal of national data opt-outs from the disclosures (see section 7 of the Compliance with National Data Opt-out Implementation Guidance)

3. Benefits

The national data opt-out delivers largely quality and societal benefits. No direct quantitative benefits have been identified as part of commissioned research by the Personalised Health and Care 2020 portfolio in 2016 and none have emerged since this review.

The national data opt-out is a policy offer on behalf of the Department of Health and Social Care and its implementation is a stated objective of the Government. Specifically, it is an enabler to increase public trust in how the NHS and other health and adult social care organisations manage confidential patient information. This trust is a vital building block to support wider digital transformation initiatives. The national data opt-out aims to increase public trust and confidence in the way that the health and care sector uses data by providing a simple, accessible way for the public to opt out of their confidential patient information being used for planning and research. These uses of data, often by national bodies or organisations that do not have a legitimate relationship to the patient are often the ones of greatest concern to the public. The national data opt-out specifically excludes individual care to avoid any potential disbenefits in terms of the patient's individual care and treatment.

The implementation of the national data opt-out generates two benefits. The table below details the benefits that are expected to be realised and which are specifically associated with the compliance with national data opt-outs across the health and adult social care sector and the primary beneficiaries.

Benefit Title	Benefit Description	Primary Beneficiary
Increased patient and carer confidence and trust by giving people choice about how their confidential patient information is being used	Patients and carers are given the ability to decide whether to share their confidential patient information for research and planning. Accurate, system wide information about this choice will be provided. Combined, this will increase confidence in NHS data sharing processes	Patients and Careers
Increased confidence of data	With the list of patients expressing a national data opt-out being held by NHS Digital, data controllers	Health and Social Care Organisations

controllers' ability to manage data flows and increased compliance with policy requirements relating to data sharing	can be confident that they have access to current opt-out preferences to enable the national data opt-out to be upheld in their data flows	and Professionals – Data Recipients

4. Timescales

The planned timeline for organisations to be compliant with the national data opt-out can be found on the compliance with the national data opt-out webpage.

It is expected that all health and adult social care organisations are required to adhere to these timeframes to be compliant with the national data opt-out operational policy and to apply patient national data opt-outs in any disclosures as required, using the service to check for national data opt-outs. Compliance with national data opt-outs is an ongoing process which organisations are required to evidence on an ongoing basis.

5. Helpdesk

For general enquires:

NHS Digital can provide help and assistance to organisations, for any queries relating to the national data opt-out or this standard. Please email:

enquiries@nhsdigital.nhs.uk

('national data opt-out' must be included within the subject title)