National data opt out policy

1. Introduction

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.
This document provides operational guidance to understand the application of national data opt-out policy for practice purposes.

A patient is able to set an opt-out via a number of channels that include online, digitally assisted and non-digital channels. Any patient with an NHS number is able to set a National Data opt-out.
The opt-out is stored in a central repository against their NHS number on the NHS Spine and is not set or visible at practice level. The National Data opt-out will also continue after the patients' death. HealthCare organisations are required to be compliant with the opt-out by March 2020 and declare their compliance on the Data Security and Protection (DSP) Toolkit.
The opt-out applies regardless of how the data is stored – electronically or paper based.

2. What are National Data Opt-Outs?

The national data opt out implements the opt-out process proposed by the National Data Guardian's Review of Data Security, Consent and Opt-Outs.
See here for more details:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF
The above review proposed the following:
"There should be a new consent/opt-out model to allow people to opt-out of their personal confidential data being used for purposes beyond their direct care".
The NDG's review carefully considered the scope of the model including its limitation to purposes beyond individual care only and for it to be an opt-out rather than consent model:
"3.2.2: The Review was persuaded that the best balance between meeting these expectations and providing a choice to those who have concerns is achieved by providing an opt-out model. The review concluded that people should be made aware of the use of their data and the benefits; an opt-out model allows data to be used whilst allowing those who have concerns to opt out".
The review also acknowledged that *"Whilst patients have a right under the NHS Constitution to request that their personal confidential data is not used beyond their direct care, there is currently no easy way for them to do that".* The national data opt-out provides a single central mechanism which gives effect to this right.

3. Applying the national data opt-out

Health and care organisations are required to apply national data opt-outs in line with the NHS National Data Opt-Out Policy.
NHS Digital has developed a technical service which enables health and adult social care organisations to check if their patients have a national data opt-out in order to enable them to comply with the opt out.

This service can be used in two ways:

- Organisations can submit a list of NHS numbers that they need to disclose and the service looks these up against the central repository of national data opt-outs. It returns a "cleaned list" of those that do not have a national data opt-out i.e. it removes the NHS numbers for those with a national data opt-out. This is most suitable for one-off and infrequent disclosures of data.

- Organisations can submit the NHS numbers for all patients with whom they have a legitimate relationship and then store temporarily the list of patients who do not have an opt-out at the current time and whose data they may be able to disclose16. There are a number of policy rules around the storage and use of this "temporary cache" of data which are set out below. This is most suitable for large scale and frequent disclosures of data.

More information on accessing the service, guidance and the timetable for the implementation of the national data opt-out through to March 2020 is provided on the National Data Opt-out Programme webpages.

Patients can apply the national data opt-out either online, post or phone. For more information see https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/.

4. What data is affected?

Broadly it is data that meets all of the following three conditions:

a) identifiable or likely identifiable (for example from other data likely to be in the possession of the data recipient);
AND
b) given in circumstances where the individual is owed an obligation of confidence;
AND
c) conveys some information about the physical or mental health or condition of an individual, a diagnosis of their condition; and/or their care or treatment.

The opt-out does not apply to data that has been anonymised in line with ICO guidance. It is also worth noting that the opt-out only applies to patient data. It covers any and all data that is disclosed for purposes beyond direct patient care.

5. Invoice Validation

Broadly, the opt-out does not apply to data used for invoice validation. Specifically, it does not apply to invoice validation for non-contracted activity. For contracted activity, anonymised data should be used.

The opt-out does not apply where a patient has given their explicit consent for the use of their data for payment and invoice validation.

Data opt-outs do not apply to data disclosed to NHS BSA for the payment of prescription charges, specifically where the data is disclosed under Regulation 18A of National Data Opt-out Operational Policy Guidance Document.

The opt-out does apply to data disclosed for payment purposes which rely on section 251 support unless it relates to non-contracted activity or specific conditions have been approved by the Confidentiality Advisory Group (CAG).

6. Risk stratification

The national data opt-out does not apply to data disclosures for risk stratification for case finding but does apply where support under Section 251 is relied upon to support the disclosure.

For the purpose of the National Data Opt-Out, risk stratification has been split into two functions, Risk Stratification for case finding and Risk Stratification for planning. Therefore the policy lines that are relevant to risk stratification are as follows:

- National data opt-outs **do not** apply to risk stratification for case finding, where carried out by a provider involved in an individual's care, as this should be treated as individual care.

- National data opt-outs **do not** apply where the data for risk stratification is anonymised in line with the ICO Code of Practice on Anonymisation.

- National data opt-outs **do** apply to data disclosures for risk stratification which rely on Section 251 support unless the standard condition requiring patient opt-outs to be respected is waived.

7. What Data is not affected?

Consent
The national data opt out does not apply where explicit consent has been obtained from the patient for the specific purpose. This can include if a patient has previously opted-out but wishes for that data to be processed for a specific purpose. The consent would override the national data opt-out and data could be processed for that specific purpose only. Other information that is applicable under the opt-out and is not covered by the explicit consent would still be subject to the opt-out if applied.

Communicable disease and risks to public health
The national data opt-out does not apply to the disclosure of confidential patient information required for the monitoring and control of communicable disease and other risks to public health.
This includes any data disclosed where Regulation 3 of The Health Service Regulations 2002 provides the lawful basis for the common law duty of confidentiality to be lifted.
See Section 251 on page 4.

Public Interest
The national data opt-out does not apply to the disclosure of confidential patient information where there is an overriding public interest in the disclosure, i.e. the public interest in disclosing the data overrides the public interest in maintaining confidentiality.

Direct Care
The national data opt-out does not apply to direct care as defined on page 5.

8. References

- The National Data Opt-out operational Policy Guidance Document
- General Data Protection Regulations (GDPR)
- Data Protection Act 2018

Appendix A: Definitions

Direct Care (Individual Care)

A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. This includes supporting individual's ability to function and improve their participation in life and society.

Data Controller

Article 4(7) of the General Data Protection Regulations (GDPR) defines the Data controller as the natural or legal person, public authority, agency or other body which, alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by the GDPR or Data Protection Act 2018

Data Processor

Article 4(7) of the General Data Protection Regulations (GDPR) defines the Data controller as the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Section 251

Section 251 of the National Health Service Act 2006 allows the Secretary of State for Health and Social Care to make regulations to authorise or require the processing of confidential patient information (CPI) for prescribed medical purposes and, in so doing, to set aside the common law duty of confidentiality. The only regulations made under this provision are the Health Service (Control of Patient Information) Regulations 2002 (SI 2002/ 1438) ("COPI Regulations").
The COPI regulations provide 3 legal gateways:

- Regulation 2 permits confidential patient information relating to patients referred for the diagnosis or treatment of cancer to be processed for the medical purposes set out in the regulation.

- Regulation 3 provides specific support for confidential patient information to be processed to diagnose, control or prevent, or recognise trends in, communicable diseases and other risks to public health. This Regulation is exempt from the national data opt - out

- Regulation 5 provides support for confidential patient information to be processed for the medical purposes set out in the Schedule, which includes 'the audit, monitoring and analysing of the provision made by the health service for patient care and treatment'.

Regulation 2 and 5 approvals from the Secretary of State or Health Research Authority are subject to advice from the Confidential Advisory Group (CAG), which is hosted by the Health Research Authority. Regulation 3 authorisations are managed by Public Health England. Any person wishing to obtain approval under Regulation 2 or 5 must to submit an application to CAG who provide independent expert advice to the relevant decision maker. A standard condition of its advice is that patient objections (i.e. opt-outs) to the use of this information are respected. It has taken a policy position that it will advise that it is not in the public interest to over-ride an opt-out in anything other than the most exceptional circumstances. For the purposes of this policy references made to Section 251 support specifically applied to regulation's 2 or 5 unless explicitly stated.

Appendix B: Version control

Version 1
Date issued: 03/02/2020
Date for review: 03/02/2023

Core document sourced from Milton Keynes CCG, with minor alterations (no change to meaning, only formatting and to correct typing errors)