

## National Data Opt Out Policy

### Introduction

The national data opt-out is a service that was introduced on 25 May 2018, enabling patients to opt out from the use of their confidential, identifiable patient information being used as data for research or planning purposes. This is in line with the recommendations of the National Data Guardian in the Review of Data Security, Consent and Opt-Outs. By September 2020 all health and care organisations are required to be compliant with the national data opt-out policy, where confidential patient information is used for research and planning purposes. NHS Digital and Public Health England are already compliant and are applying national data opt-outs. Patients can view or change their national data opt-out choice any time, by visiting [www.nhs.uk/your-nhs-data-matters](http://www.nhs.uk/your-nhs-data-matters)

### Background

The National Data Opt-out Programme (NDOP) is a product of the data security review by the National Data Guardian on how individuals' data is used and shared by healthcare organisations. It is part of a vision to improve patients' trust and confidence in how data is looked after by the health and social care system. The National Opt-out ties in with other work on data security and ensuring data is only used for the benefit of people's health and care. NDOP has been created to provide a model that will allow each individual patient to have control over specific data, being able to choose the purposes for which data can be shared.

Type 2 opt-outs A "Type 2" opt-out was introduced in 2014 to allow patients who did not want their confidential patient data to be used beyond NHS Digital to register this objection with their GP. Previously there were two ways in which a patient could opt out of sharing their personal information:

- A type 1 opt out prevents information being shared outside a GP practice for purposes other than direct care.
- A type 2 opt out prevented information being shared outside NHS Digital for purposes beyond the individual's direct care. From 25 May 2018 the type 2 opt-out has been replaced by the national data opt-out.

Type 2 opt-outs that were recorded on or before 11 October 2018 have been automatically converted to national data opt-outs. The opt-out allows patients to directly express a preference to opt out of using their personal identifiable information for;

- Health Planning – e.g. data used to improve delivery of services
- Health Research – e.g. finding ways to improve treatments

### Choosing to opt out

NDOP will provide a means for patients who are registered with a GP in England to make an informed choice and have control how their patient data is shared. The initial phase will provide an on-line portal where patients can use a standard web browser to set their data sharing preferences. Additional mechanisms will be introduced at a later date, including GP Practice Systems, mobile devices and off-line systems. Patients who decide they do not want their personally identifiable data used for planning and research purposes will be able to make their choice online. The NHS will provide a non-digital alternative for patients who can't or don't want to use an online system.

- Patients can change their mind anytime.
- Existing Type 2 opt-outs (the option for a patient to register with their GP, to prevent their identifiable data leaving NHS Digital) will be converted to the new national data opt-out.

- Patients with type 2 opt-outs will be informed of this change individually. Information for health and care professionals For primary care, the introduction of the national data opt-out will mean you have two new areas of responsibility;
- You will need to be aware of the service in case patients ask you about it
- You will be expected to uphold these preferences and advise patients.

### **What the national data opt out applies to**

The opt-out relates to information about an individual's health and adult social care provided in England only. It will not apply to information flowing from outside England (this includes from the other home nations) directly to a research or planning body. However, when information from another home nation comes into a GP surgery (where the opt-out applies), then it is subject to the national data opt-out restrictions.

- information about the deceased as the GDPR only applies to living individuals.
  - Any confidential patient information generated or processed by a health or adult social care organisation within England
  - Confidential patient information held by other organisations relating to care provided or co-ordinated by a public body
- Any disclosure of data for purposes beyond individual care The opt-out will apply unless:
  - the patient has consented to a specific data use
  - the data is required by law
  - where there is an overriding public interest for the disclosure
  - the data is anonymised in line with the ICO code of practice on anonymisation
  - a specific exemption has been granted.

### **Opt-outs from other UK countries**

Opt-outs offered in Wales, Scotland (the "Spire Opt-out"), Northern Ireland, or the Isle of Man (IoM) or the Channel Islands do not apply in England – but they may be applied prior to receipt of any data in England. Opt-outs that are implemented in other countries are for a specific purpose, but this does not mean they apply in England.

### **When the data opt-out will not apply**

**Risks to Public Health** It doesn't apply if disclosing confidential patient information is needed for risks to public health, such as monitoring and control of communicable diseases. This includes where there is a lawful basis for lifting the common law duty of confidentiality (Public Health England (PHE) oversees the use of this legal process).

**Regulation 3 of The Health Service (Control of Patient Information) Regulations 2002** allows Lawful processing of confidential patient information This can be lawfully processed for the following reasons;

- diagnosing communicable diseases and other risks to public health
- recognising trends in such diseases and risks
  - controlling and preventing the spread of such diseases and risks
- monitoring and managing:
  - o outbreaks of communicable disease
  - o incidents of exposure to communicable disease
  - o the delivery, efficacy and safety of immunisation programmes
  - o adverse reactions to vaccines and medicines
  - o risks of infection acquired from food or the environment (including water supplies)
  - o the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease.