**Dr Nagpals Surgery**

 **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 2021 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.

The Health and Social Care Act 2012 gives NHS Digital statutory powers to require data from health or social care providers in England where NHS Digital has been directed to do so by the Department of Health (on behalf of the Secretary of State for Health) or NHS England.

The Department of Health has directed NHS Digital to perform this work making it mandatory.

NHS Digital will collect data at the level of the individual patient (that is: record level data). This will involve a separate row of data being returned for each individual patient.

NHS Digital will collect personal data in the form of patients' NHS Numbers.

The NHS Number is a unique number used to identify patients and match them to their health records. It is an identifiable, personal data item.

No other personal data items, such as Name, Address, Postcode or Date of Birth, will be collected. Similarly, no sensitive data items, such as Ethnicity, Sexual Orientation or Physical or Mental Health Conditions, will be collected.

# 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.

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.

Individuals who wish to opt-out of this data collection should contact their general practice in order to register a **Type 1 opt-out**. This is an objection that prevents an individual's personal confidential information from being shared outside of their general practice except when it is being used for the purposes of direct care, or in particular circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease.

NHS Digital will uphold Type 1 opt-outs in collecting these data from general practices (that is: any patients who have registered a Type 1 opt-out prior to the point in time at which this data collection takes place will not be included in this data collection).

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. This type of opt-out is an objection that prevents an individual's personal confidential information from being shared outside of NHS Digital, except when it is being used for the purposes of direct care. Type 2 opt-outs do not apply to this data collection as no personal data will leave NHS Digital. Instead, the information that is reported back to GPs and general practices will include percentages (and associated counts) of patients who fall into each of the metrics.

Patients can change their mind anytime.

Further information is available on the [keeping patient data safe](https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe) page.

# 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:
	+ 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
	+ risks of infection acquired from food or the environment (including water supplies)
	+ the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease.

**Overriding Public Interest**

Opting out does not apply to disclosure of information where there is an overriding public interest in the disclosure, such as;

* reporting of gun and knife wounds in line with GMC guidance, and
* patients' fitness to drive and reporting concerns to the DVLA or DVA in line with GMC guidance

Data controllers should have their own arrangements in place to apply a ‘public interest test’ as and where necessary.

**Required by Law / court order**

Examples of disclosures required by law.

* CQC Inspect & entry requirements
* NHS Digital collecting information as directed by the Secretary of State or NHS England
* NHS Counter Fraud Service requests in order to prevent, detect and prosecute NHS fraud
* professional regulators investigating fitness to practise (e.g. GMC, NMC)
* Coroners’ investigating the circumstances of a violent death, or death in custody
* Health professionals reporting notifiable diseases, including food poisoning
* Chief Medical Officer must be notified of termination of pregnancy
* Employers reporting deaths, major injuries and accidents to the Health and Safety Executive
* Providing information to the police when requested if an offence has been caused
* Prevention of terrorism or prosecuting a terrorist under Terrorism Acts
* Child or vulnerable adult safeguarding purposes (e.g. s.47 Children Act 1989);
* Cases of female genital mutilation to police (Female Genital Mutilation Act 2003)
* Court order from a judge or presiding officer of a civil or criminal court
* information reported to HFEA for inclusion on the register of assisted reproduction and fertility treatments (Human Fertilisation and Embryology Act 1990
* Some disclosures to the Office of National Statistics
* Information relating to transplant approvals
* Providing information to Responsible bodies including health boards, trusts and regulatory bodies relating to the management and use of controlled drugs

This is not an exhaustive list, so information governance and/or legal advice should be sought where necessary.