Document filename:	**NDOPNationalDataOptOutPolicy_v3.0**		
Project / Programme	**National Data Opt-out Programme**	Project	**Policy Implementation Workstream**
Status	**Final**	Version	**3.0**
		Version issue date	**04/03/2019**

National Data Opt-out Operational Policy Guidance Document

Version 3.0

Document management

Revision History

Version	Date	Summary of Changes
2.0	25/5/18	Published for public beta
2.1	1/10/18	Minor updates
3.0	4/3/19	Major update for implementation

Approved by

This document must be approved by the following groups:

Name	Title	Date	Version
Programme Head	NDOP Programme Head, NHS Digital	Dec 2018	3.0
Programme Board	National Data Opt-out Programme Board	Jan 2019	3.0
DHSC	Department of Health and Social Care	Feb 2019	3.0

Document Control:

The controlled copy of this document is maintained on the National Data Opt-out Programme webpages. 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

Executive summary

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 – it sets out when the national data opt-out must be applied along with the exemptions when it will not apply. The national data opt-out applies to data that originates within the health and adult social care system in England and is applied by health and care organisations that subsequently process this data for purposes beyond individual care. The opt-out does not apply to data disclosed by providers of health and care services outside of England or to children's social care services. This document includes guidance in relation to several specific data uses, for example risk stratification.

The national data opt-out is aligned with the authorisation used for sharing a patient's data in accordance with the common law duty of confidentiality (CLDC). In broad terms the national data opt-out applies unless there is a mandatory legal requirement or an overriding public interest for the data to be shared. The opt-out does not apply when the individual has consented to the sharing of their data or where the data is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice on Anonymisation.

A member of the public is able to set an opt-out via a number of channels that include online, digitally assisted and non-digital channels. Any person registered on the Personal Demographic Services (PDS) and who consequently has an NHS number allocated to them is able to set a national data opt-out. The opt-out is stored in a central repository against their NHS number on the Spine[1].

NHS Digital and Public Health England are applying the national data opt-out to any in scope data releases and are compliant with this policy. Other relevant organisations are required to be compliant with the opt-out by March 2020.

The opt-out applies regardless of the format of the data and this includes structured and unstructured electronic data and paper records. When the opt-out is applied, the entire record (or records) associated with that individual must be fully removed from the data being disclosed. The NHS number is used as the identifier for the removal of the records.

A national data opt-out publication provides statistics on the national data opt-out against various dimensions, including age and geography to help organisations to understand the impact of the opt-out on their data. Related documents that set out requirements and guidance on the application of the national data opt-out include the Data Security and Protection Toolkit (DSPT), the forthcoming Information Standard on Compliance with the National Data Opt-out and the NHS Digital Code of Practice on Confidential Information. Further information and guidance on the opt-out is available from the national data opt-out programme webpages.

[1] Spine supports the IT infrastructure for health and social care in England.

1 Introduction

1.1 Document Purpose

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.

1.2 Audience

The intended audience for this document comprises both individuals who are responsible for ensuring that the legal obligations of data protection and confidentiality are met and implemented and also those who are processing patient data within health and adult social care organisations. The former group may include the information governance lead, Caldicott Guardian, data protection officer, chief information officer, chief clinical information officer, senior information risk owner and others responsible for data protection and compliance. The latter group may include information analysts and data processing staff. In essence this includes anyone who is responsible for the processing or handling of patient data and, therefore, may be required to apply the national data opt-out policy.

This document may also be of interest to researchers, members of the public or healthcare professionals who have a particular interest in this subject although other more suitable materials are available on the national data opt-out programme website.

This document is not intended to support members of the public in setting national data opt-outs or health and adult social care professionals in providing guidance or signposting to the public. Other resources for this purpose are provided on the:

- national data opt-out service webpages - information to support the public to make an informed decision and to set a national data opt-out
- national data opt-out programme webpages – factsheets, guidance and resources for health and care professionals.

1.3 Scope of this document

This document provides practical operational guidance based on the national data opt-out policy as set by the Department of Health and Social Care (DHSC). NHS Digital is directed to produce and maintain this guidance.

This document is a comprehensive articulation of the policy rules relevant to considering and applying national data opt-outs.

This document does not provide detailed guidance relating to the interpretation of some of the underpinning concepts relied upon within this document, for example what is individual care or what is deemed to be anonymised data in line with the ICO Code of Practice. However, it does signpost to existing guidance as appropriate.

This guidance is reviewed regularly in order to ensure that it remains up to date as the national data opt-out is implemented across the health and care system. It is a controlled document and users should always refer back to the version published online to ensure that they are using the most up to date version.

1.4 Terminology

A full list of abbreviations is provided in Appendix 1: Abbreviations. Appendix 2: Definitions defines some of the key terms which are used in this document. For consistency and to aid understanding the following terminology is used throughout this document with the specific meaning as set out below:

- “individual care” this is often referred to as ‘direct care’ where legally the sharing of data is based on implied consent, i.e. where the patient knows or would reasonably expect their data to be shared for their care and treatment. The definition of individual care is set out in Appendix 2: Definitions. For completeness the definition of indirect care is also included here.
- “purposes beyond individual care” is used to refer to all other uses of data outside an individual’s care and treatment. This is sometimes also referred to as “secondary uses”, “indirect care" or “other purposes”.
- “data disclosure” this is the term used to describe sharing of data in relation to the common law duty of confidentiality and is used to indicate the point at which the national data opt-out must be applied.
- “apply” and “applying” is used to describe the process whereby organisations respect national data opt-outs in any data disclosures, this may sometimes be referred to as “upholding”.
- “compliance” is used to refer to an organisation having assessed its data flows to determine whether they fall within the scope of national data opt-out policy (as defined by this document), and applying the national data opt-outs as necessary to any flows that are within scope. An organisation may be in compliance even if it is not applying the national data opt-out where it does not have any data disclosures that need the opt-out to be applied. For example where it is processing data for individual care only.
- “Common law duty of confidentiality” (CLDC) is used to refer to the common law regarding information that is subject to a duty of confidence. This is sometimes termed the “common law duty of confidence”.
- “patient” is used to refer to people in the context of an opt-out being applied to any “data disclosure”. In some parts of the health and care system the term “client” or “service user” may be equivalent.
- “data protection legislation” is used in this document as an umbrella term to cover the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR), and any regulations which relate to the DPA or GDPR.

2 What are national data opt-outs?

2.1 Context

The national data opt-out implements the opt-out model proposed by the National Data Guardian, as accepted by the Government and directed by the Department of Health and Social Care.

The National Data Guardian's Review of Data Security, Consent and Opt-Outs (NDG Review) proposed that:

"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"*[2]. The national data opt-out provides a single central mechanism which gives effect to this right.

The Government undertook a public consultation before publishing its response to the NDG review which accepted all the recommendations made by the National Data Guardian.

2.2 Type of data

The national data opt-out applies to "confidential patient information" (CPI) and guidance is provided for health and care professionals in assessing what is CPI for the purposes of applying the national data opt-out. CPI is defined in section 251 (11) of the National Health Service Act 2006. Broadly it is information that meets all of the following 3 requirements:

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.

It should be noted that Section 251 (also known as S.251) has been updated to ensure that the definitions used expressly include local authority social care (i.e. care provided for, or arranged by, a local authority). The term confidential patient information (CPI) also covers data which falls within the "special categories of personal data" under article 9 GDPR and indeed goes beyond this as it also covers information about the deceased as the GDPR only applies to living individuals. Further information on assessing what is CPI for the purposes of applying the national data opt-out is provided in Appendix 6: Confidential Patient Information (CPI) definition.

[2] It should be noted that the NHS Constitution does not provide an absolute right to stop confidential patient information flowing and it does not apply to social care.

The national data opt-out does not apply to information that is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice (CoP) on Anonymisation or is aggregate or count type data. It should be noted that the ICO Code of Practice covers a range of anonymised data including aggregate data for publication to the world at large through to de-identified data for limited access. De-identified data for limited access requires a suite of additional organisational and technical control measures to ensure that the risk of re-identification is remote, for example access controls, purpose limitation, staff confidentiality agreements, contractual controls etc.

For clarity the national data opt-out is for patient data only and applies to confidential patient information - the national data opt-out does not apply to workforce or staff data. NB: Staff data may be removed as a result of the opt-out being applied but only where it is relevant to a patient's care (for example, a consultant's name may be linked to an episode of care). Staff data, and any other personal data which is not confidential patient information, would still be subject to data protection legislation and the rights provided under this, including article 21 (right to object) in GDPR, but sits **outside** of the scope of the national data opt-out[3].

2.3 Purpose and point of application

The national data opt-out is defined based on purpose and applies to any disclosure of data for purposes beyond individual care. More specifically:

- The national data opt-out would **always** need to be considered to be applied (in line with this policy) at the organisational or data controller boundary.
- The national data opt-out **may** also need to be considered to be applied internally at the point of change of purpose – specifically where S.251 support is relied upon as the legal basis for allowing the disclosure of confidential patient information.

Purposes beyond individual care are defined as anything that does not meet the definition of individual care (see Appendix 2: Definitions). It would include purposes such as planning for the provision of local services, managing and running NHS and adult social care services, commissioning, invoice validation, national clinical audits and research. For completeness the definition of indirect care is also included in the appendix which will assist organisations in making the decision about whether a particular use falls outside of the definition of individual care.

The NDG review made it clear that there are some elements of individual care which rely on the processing of data nationally, for example the electronic transfer of prescriptions, screening, immunisation programmes and the Summary Care Record. *"The Review heard no evidence to suggest that there should be a change to effective local or national arrangements for sharing information."* These purposes are considered to be for individual care and are not subject to the national data opt-out.

2.4 Legal framework and lawful basis

The national data opt-out is a policy opt-out that must be considered and applied alongside existing data protection legislation, other laws and best practice. These include data protection legislation and the CLDC, Human Rights Act 1998, and all relevant Codes of Practice such as the DHSC and NHS Digital codes of confidentiality and best practice guidance, for example the seven Caldicott principles.

[3] Information provided by occupational health services would be considered to be relevant to an individual's care and potentially in scope of the national data opt-out.

Data protection legislation (DPA 2018 and GDPR) requires data controllers to ensure that all processing of personal data is in line with the principles including being fair, lawful and transparent. This includes ensuring compliance with the CLDC.

To remain lawful data controllers must ensure:

- An Article 6 condition is satisfied (for personal data); and
- An Article 9 condition is satisfied (as health data is a special category of data)
- and compliance with the common law requirements (CLDC), for example there is consent or some other statutory authorisation for the data use such as S.251

These underpinning legal requirements are required now, remain in place and the introduction of the opt-out does not alter or amend this. This policy is based on the assumption that organisations already have effective processes and procedures in place to ensure that their data processing is lawful and appropriate.

Data controllers need to be clear **first on the purpose** for the disclosure - is it:

- for individual care – in which case the opt-out **does not** apply OR
- another purpose beyond individual care and the opt-out **may apply.** This will depend upon how the **common law requirement on confidentiality (i.e. CLDC) is being satisfied**

A lawful basis is needed for data protection legislation including the CLDC. Data protection legislation requires the lawful basis for any processing to be communicated clearly to individuals through appropriate channels and materials in line with the duty of transparency.

Once the lawful basis for the processing has been established then the application of the national data opt-out can be determined based on the authorisation for complying with the CLDC.

The table below summarises the commonly used bases and sets out when the opt-out applies. Options include the use of the legal gateways set out in the Control of Patient Information Regulations 2002 (made under Section 251 of the NHS Act 2006) which allow confidential patient information to be used without patient consent:

Legal basis in common law	Opt-out applies	Comments
Common Law Consent (Implied):	No – out of scope for the national data opt-out	For common law purposes the sharing of information for direct or individual care purposes[4] is on the basis of implied consent. This is out of scope for the national data opt-out - which only applies to purposes beyond individual care. N.B. This is included in this table for completeness and to emphasise that implied consent can only be used when the surrounding circumstances mean that a patient knows, or would reasonably expect, that their data will be shared. In other words there should be 'no surprises' for the individual about who has had access to information about them where implied consent is relied upon.
Common Law Consent (Explicit):	No	In this case an individual has given their consent for a specific use of their data, for example consenting to participate in a research study. This would fall within the general exemption from the national data opt-out (see 2.5 below). This rule applies even if the consent was given before the patient had set a national data opt-out.
Mandatory legal requirement	No	Where there is a legal requirement for the data disclosure that specifically sets aside the common law duty of confidentiality then the national data opt-out will not apply.
Section 251 Regulation 2 – for diagnosis and treatment of cancer Regulation 5 – for the medical purposes set out in the schedule to the regulations	Yes – in general **BUT** there are some specific exemptions	Data disclosure has Section 251 support obtained under regulation 2 or 5. This applies unless CAG have advised: a) that the national data opt-out is overridden in the public interest (NB: This would be in exceptional circumstances only) or b) a different opt-out can apply and the section 251 decision-maker (Secretary of State for Health and Social Care or Health Research Authority) has agreed to this. For example data disclosures to Public Health England (PHE) for the National Cancer Register or the National Congenital Anomaly and Rare Diseases Register. NB: Where reference is made to Section 251 (S.251) support in the rest of this document it

[4] An individual will still be able to ask their doctor or other healthcare professional not to share a particular piece of information with others involved in providing their care and should be asked for their explicit consent before access to their whole record is given.

Legal basis in common law	Opt-out applies	Comments
		specifically applies to regulation 2 or 5 unless explicitly stated otherwise. Please see Policy considerations for specific organisations or purposes for specific cases where this may not apply.
Section 251 Regulation 3 – for communicable diseases and other risks to public health	No	Data disclosure under Regulation 3 of the Control of Patient Information Regulations 2002 is exempt from the national data opt-out.

Hence when determining if national data opt-outs will apply this requires the following to be clearly established:

- Purpose - it is for a purpose beyond individual care and
- The basis for the disclosure in common law - the national data opt-out applies where S.251 support is relied upon.

Further guidance on lawful processing under GDPR has been published by the Information Governance Alliance and should be read in conjunction with this operational policy guidance. Further information on patient confidentiality is available in "Confidentiality: NHS Code of Practice" published by DHSC and the "Code of practice on confidential information" published by NHS Digital.

2.5 Patient Consent

The national data opt-out does not apply where a patient has given their explicit consent to the specific use of their data.

The use of consent for specific purposes is supported by the following excerpt from the NDG review:

"People should continue to be able to give their explicit consent separately if they wish, e.g. to be involved in research, as they do now. They should be able to do so regardless of whether they have opted out of their data being used for purposes beyond direct care. This should apply to patients' decisions made both before and after the implementation of the new opt-out model".

As the NDG specified there is no dependency on the timing of when a person gave their consent for a specific disclosure of their data. **A person may give consent for a specific purpose either before or after setting a national data opt-out and this consent will constitute an exemption from the national data opt-out.**

Further guidance on consent under new data protection legislation (GDPR) has been published by the Information Governance Alliance and should be read in conjunction with this operational policy guidance.

2.6 Geographical coverage

The national data opt-out relates to information about an individual's health and adult social care provided in England.

It does not apply to information about an individual's health or care which is generated or processed outside of England including in home countries of the UK, that is Wales, Scotland, Northern Ireland, or the Isle of Man or Channel Islands.

Opt-outs offered in other home countries[5] for example 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.

National data opt-outs continue to apply until the individual proactively changes their opt-out preference, including where the individual subsequently moves away from England. For example an individual moving from England to Wales who has a national data opt-out but does not remove it when they move – their opt-out remains in place and is applied in line with this policy.

The policy for applying national data opt-outs to data flows outside of England are outlined in Cross border data flows.

2.7 Interaction with other opt-outs

Prior to the launch of the national data opt-out individuals could set two types of general opt-outs, via their GP practice:

- A type 1 opt-out prevents information that identifies individuals being shared outside of their GP practice, for secondary uses.
- A type 2 opt-out prevented confidential patient information from being shared outside of NHS Digital for purposes beyond individual care.

Type 1 opt-outs continue to be honoured until 2020 when the Department of Health and Social Care (DHSC) will consult with the NDG before confirming their removal.

Type 2 opt-outs have been replaced by the national data opt-out and are no longer valid. All type 2 opt-outs recorded in GP practices up to and including 11 October 2018 have been migrated to become national data opt-outs. NHS Digital has written to inform people who previously registered a type 2 opt-out of this change. More information on the conversion of type 2 opt-outs can be found on the NHS Digital website.

Other national and local opt-outs for specific purposes (for example summary care record opt-out) remain in place and should continue to be applied, when appropriate, alongside the national data opt-out.

There are specific arrangements for the opt-outs that apply to data flows to Public Health England (PHE) for the two national disease registries and screening programmes that they operate. These are set out in Flows to Public Health England National Disease Registers and Population screening programmes. Other specific arrangements are in place for Assuring Transformation and for National patient experience surveys.

[5] Opt-outs implemented within other countries, such as the Spire Opt-out in Scotland, are for a specific purpose and applicable only within the laws and regulations of that country and therefore must not be inferred as being the equivalent of a national data opt-out within England.

2.8 Compliance with national data opt-out policy

NHS Digital and Public Health England are applying the national data opt-out to any in scope data releases and are compliant with this policy. Other relevant organisations are required to be compliant with the national data opt-out by March 2020.

Further details of the timelines for compliance with the national data opt-out are available on the national data opt-out programme website.

2.9 Deceased patients

A national data opt-out continues to be maintained and applied for an individual after they have died. Health and adult social care organisations are expected to continue to apply opt-outs for deceased patients and their opt-out will continue to be held on the Spine repository.

3 Setting an opt-out

3.1 The question wording

The national data opt-out is based on a single question that covers all uses of data beyond individual care. Individuals are provided with information about the national data opt-out to enable them to make an informed decision and are required to verify their identity prior to being presented with the opt-out question:

Your confidential patient information can be used for improving health, care and services, including:

- *planning to improve health and care services*
- *research to find a cure for serious illnesses*

Your decision will not affect your individual care and you can change your mind anytime you like.

I allow my confidential patient information to be used for research and planning

This question was developed and tested with the public to ensure that they understood the choice being made.

3.2 Who can opt out

Any person registered on PDS (and consequently with an NHS number allocated to them) is able to set a national data opt-out. This covers the majority of patients who have received health or care services in England and, therefore, have data about them in the health and care system in England.

Children under 13[6] and those who lack capacity are not able to set an opt-out themselves. In these cases, individuals who have a formal, legal relationship to act on behalf of them (i.e. somebody who has parental responsibility, a lasting power of attorney or court appointed deputy) are able to set an opt-out on their behalf by proxy. Special arrangements are also in place to ensure that those detained in prisons and secure settings and those where their record is marked as “sensitive” are able to set an opt-out if they wish to.

An Equality Impact Assessment (EIA) has been undertaken to ensure that no groups are disadvantaged by the national data opt-out. This is published on the national data opt-out programme webpages.

3.3 Channels to set a national data opt-out

A number of different channels are available for the public to set a national data opt-out. These are:

- a digital (online) channel accessed via the national data opt-out service.
- for those who need support to set their national data opt-out preference online a digitally-assisted channel is provided that enables members of the public to set a national data opt-out with assistance from NHS Digital staff via the national helpline.
- a non-digital (paper based) channel accessed by the national helpline or through forms which can be printed from the webpages, and
- via the NHS App as this becomes available.

[6] A child is able to set their own opt-out from age 13 which aligns with the minimum age at which children can give their consent to participate in digital services as set out in data protection legislation. This is not based on any test of competence.

There are some points that apply to specific groups with respect to setting a national data opt-out:

- Individuals aged 13 or over are able to set a national data opt-out via the digital, digitally-assisted and non-digital channels.
- Those with parental responsibility[7] are able to set a national data opt-out on behalf of a child under the age of 13 via the non-digital channel only. There is a specific form that allows a choice to be set for up to 6 children at once. Any national data opt-out that has been set by a person with parental responsibility for a child under the age of 13 will remain in place unless and until it is proactively changed.
- Those who have a formal proxy relationship to make decisions on behalf of another adult (either a lasting power of attorney or a court appointed deputy) are able to set a national data opt-out on behalf of that person via the non-digital channel only.
- Individuals in the secure and detained estate (e.g. prisons) are able to set a national data opt-out through the healthcare professionals working in these settings.
- Individuals who have agreed with their GP for their records to be marked as sensitive will be offered the choice to set a national data opt-out through the established processes to set (or remove) a sensitive flag.

A national data opt-out is stored against a person's individual record on the NHS Digital Spine against their NHS number.

In some circumstances individuals may be allocated a new NHS number. The rules of how any existing national data opt-outs are applied to the new NHS number and in relation to other changes of circumstances are outlined in Appendix 4: Changes to NHS number.

[7] Parents and legal guardians

4 Which organisations does the opt-out apply to?

The NDG review states *"This opt-out will be respected by all organisations that use health and social care information"*. The following sub-sections define the organisations to which the opt-out will apply:

4.1 Health and adult social care system

The national data opt-out applies to data that originates within the health and adult social care system in England. The following organisations are considered to be part of the health and adult social care system in England and must consider whether they are required to apply the national data opt-out:

- Department of Health and Social Care and other national bodies e.g. NHS England
- NHS 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.

This definition is aligned to the Health and Social Care Act Section 250 which is the definition of organisations required to have regard to published information standards. Such organisations need to assess whether any of their data disclosures require the opt-out to be applied – some organisations may not have any data uses that are in scope.

4.1.1 Specific Inclusions

For the avoidance of doubt confidential patient information generated or processed in the following organisations and services must consider national data opt-outs when processing data for purposes beyond individual care in line with the wider policy:

- health service providers including NHS foundation trusts and trusts, mental health and community trusts, ambulance trusts, primary care providers including GPs, dentists, ophthalmic services and pharmacists
- private providers including Any Qualified Providers (AQPs) who provide health and adult social care services which are funded or under contract with a public body, for example NHS England, CCG or local authority)
- Defence Medical Services (DMS)
- Healthcare services provided across the secure and detained estate (e.g. prison healthcare)
- public health including local authority public health functions and public health providers, for example school nursing
- adult social care services including care that is arranged or provided by local authorities and adult social care providers (i.e. where this is regulated by the Care Quality Commission (CQC)) (see below for Children's Social Care), and
- any other organisation who handles and discloses health and adult social care information as a data controller including commissioners, for example Clinical Commissioning Groups (CCGs) or national bodies, for example Department of Health and Social Care, NHS Digital, NHS England, Public Health England (PHE), Health Education England, National Institute for Health and Care Excellence, Medicines and Healthcare Products Regulatory Agency, Care Quality Commission (CQC), NHS Improvement, , NHS Business Services Authority (NHS BSA), NHS Shared Business Services (NHS SBS), NHS Resolution, NHS Blood and Transplant, Human

Fertilisation and Embryology Authority, Human Tissue Authority, Health Research Authority, NHS Counter Fraud Authority and Healthcare Safety Investigation Branch.

4.1.2 Specific Exclusions

The following organisations and services are not part of the health and adult social care system in England. National data opt-outs, therefore, do not apply to information relating to individuals originating within the following organisations:

- providers of health, public health or adult social care services outside of England
- 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 e.g.
    - assessments for disability or other benefits purposes carried out independently of the health and adult social care system (typically by the Department for Work and Pensions - DWP)
    - coroners' reports (coroners fall under the remit of Home Office)
    - health assessment carried out by the Courts/legal service
    - Her Majesty's Revenue & Customs
    - health assessments undertaken privately for pension providers or insurance companies[8]
    - universities, and
    - Office for National Statistics (ONS) / General Registrar's Office (GRO)
    - occupational health assessments

The national data opt-out does not apply to organisations that do not generate health and adult social care data but where such data is lawfully disclosed to them for individual care purposes only (for example, charities who provide day care services for patients).

Research organisations such as Universities may receive confidential patient information and the health and adult social care organisation releasing the data may be required to apply national data opt-outs depending on the legal basis for the data disclosure (typically Section 251 support). However, the national data opt-out will not apply to any health-related data that is generated solely within such organisations for research purposes e.g. tests undertaken by research staff as part of a clinical trial.

These research organisations would not usually be required to apply national data opt-outs to any data disclosure. However, a possible exception where they may be required to do so would be via a condition within a Data Sharing Agreement (DSA), for example if health and adult social care information may be onwardly disclosed.

National data opt-outs may apply to data originating from such organisations when the data disclosure is by data controllers within the health and adult social care system in England. For example where tests undertaken privately are then added to a patient's GP record.

4.2 Privately funded health and care

The national data opt-out applies to data relating to publicly funded or arranged care only (for example, a local authority may still arrange a patient's care even though it is provided by a private provider and the patient is fully or partially funding the care themselves). By extension, the national data opt-out does not apply to data related to

[8] These are also undertaken with consent from the individual

private patients at private providers or to patients at a charitable provider unless (as previously noted) the care is being funded or has been arranged by a public body such as a local authority. This is summarised as:

In scope

- All NHS organisations (including private patients treated within such organisations)
- Adult social care which is funded or arranged by a public body (typically a local authority)
- NHS arranged care within private providers (e.g. Nuffield, BMI Healthcare)
- Any release of data by NHS Digital which relates to private patients including that which is collected by a request under S259 of the Health and Social Care Act 2012 (HSCA)

Out of scope

- Privately (non-NHS) funded patients within private providers unless the care is funded or co-ordinated by a public body
- Care which is not provided or co-ordinated by a public body, that is privately arranged/privately funded care

It is of note that in adult social care, providers typically have a range of patients receiving both publicly funded and arranged care and privately funded and arranged care in the same care setting (typically a care home). The funding arrangements for individual patients may also change several times over short time periods. Providers who fit such a model may choose to voluntarily extend the national data opt-out to cover all their patients in order to make implementation within their setting more straightforward. This voluntary extension of the model would need to be made clear to their patients via privacy notices and other information provided.

4.3 Data controllers and processors

Data controllers, whether solely or jointly with another organisation, are responsible for ensuring that national data opt-outs are applied in line with this policy.

In some cases this will require data controllers to instruct any organisations acting as a data processor under their instruction to apply the national data opt-out.

In line with wider legal requirements data processors must comply with instructions from the data controller in relation to the national data opt-out.

Data controllers must apply national data opt-outs whenever confidential patient information is to be disclosed outside of their data controllership boundary in line with the wider policy (see figure 1 below). Data controllers may also need to apply national data opt-outs for internal uses of the data where the purpose changes from individual care and the disclosure is relying on S.251 support to be lawful.

Further information on the responsibilities of data controllers is provided by the IGA.

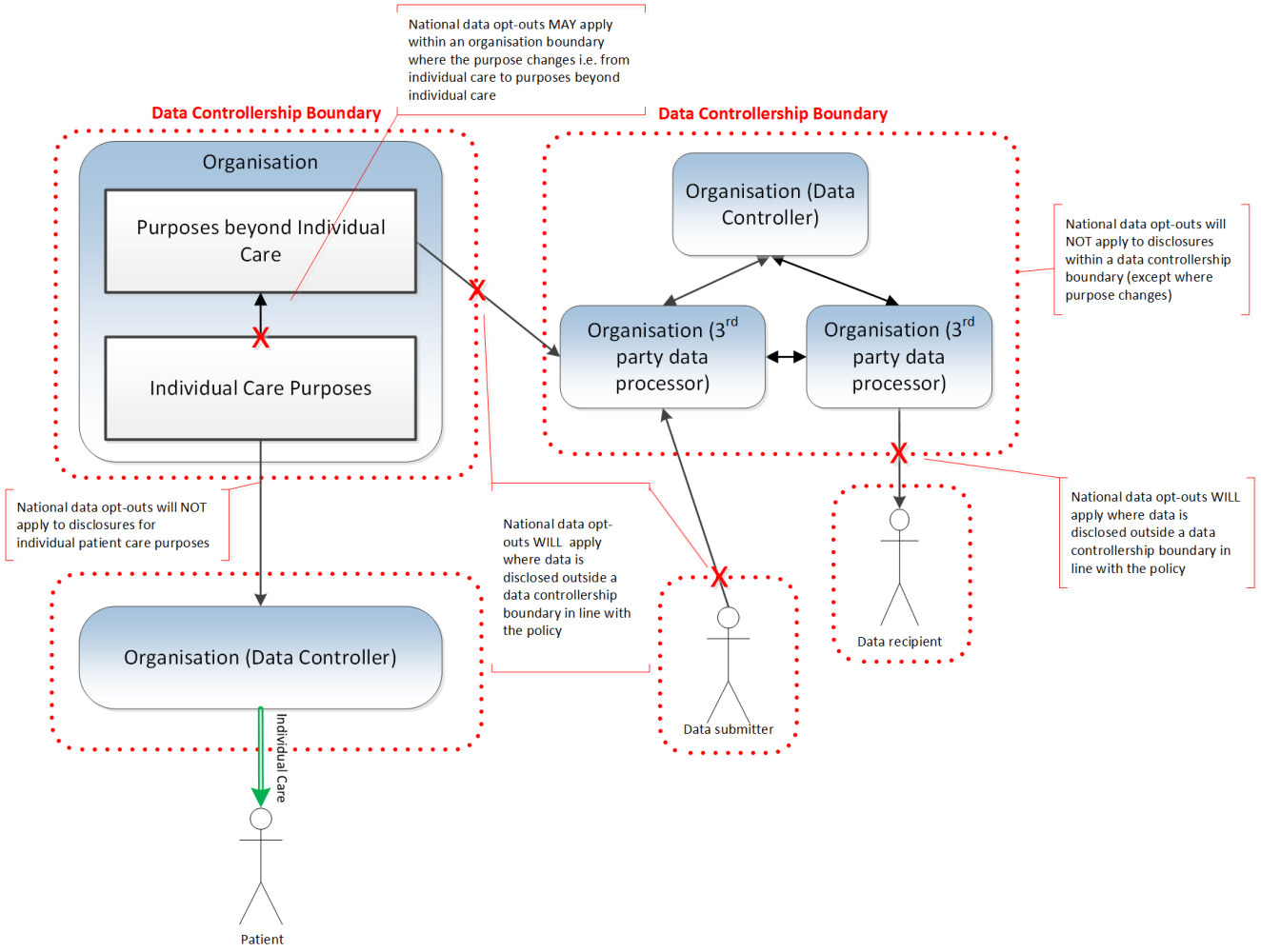

Figure 1: Application of national data opt-outs within both data controller and organisational boundaries

5 When does a national data opt-out apply?

5.1 Disclosures using S.251 - Regulation 2 and 5

National data opt-outs apply to the use of confidential patient information approved under:

- **regulation 2 (medical purposes related to the diagnosis or treatment of neoplasia) or**
- **regulation 5 (general medical purposes)**

of the Health Service (Control of Patient Information) Regulations 2002.

National data opt-outs apply in cases where the approval is subject to the Confidentiality Advisory Group (CAG)[9] 'standard condition' that a patient's wishes regarding this use of information about them (i.e. their opt-out) is respected. In exceptional circumstances, and on a case-by-case basis only, CAG may advise the decision-maker that the national data opt-out should not apply to a specific data flow supported under S.251. It is the responsibility of the data controller to satisfy themselves that such an exemption from the standard condition has been given e.g. by requesting sight of the S.251 approval letter or published minutes which should clearly indicate that opt-outs do not apply before they disclose any data.

CAG consider a large number of section 251 applications each year, the CAG Registers give details of approvals under section 251 (regulation 2 and 5) which cover both non-research and research applications. Specific exemptions to this are set out in Section 7 - Policy considerations for specific organisations or purposes. Where these are still subject to the standard CAG condition, there will need to be an alternative opt out procedure[10].

CAG may, as part of their consideration of an application, also recommend that a local or study-specific opt-out is applied in addition to the national data opt-out. This allows an individual to opt out from the CAG-approved study only without having to register a national data opt-out that would prevent all uses of their data for planning or research. This is particularly important during the transition period from May 2018 through to March 2020 when the functionality for other organisations across health and care to uphold the opt-out is still being rolled out. However, CAG reserve the right to recommend an additional opt-out in some specific circumstances after the full introduction of the national data opt-out, for example where an application is for a research study which draws data from a wider geography (for example England and Wales) or where the confidential patient information is particularly sensitive.

For avoidance of doubt where the approval for access to the data relies upon S.251 (regulation 2 or 5) support then all data disclosed under this approval will be deemed to be confidential patient information even where the specific disclosure does not contain any health or care information.

5.2 Data format

National data opt-outs apply to data disclosures involving confidential patient information for purposes beyond individual care regardless of the data format. The national data opt-out applies to structured electronic data (for example csv, XML), unstructured electronic data (for example PDFs, scans or images) and paper records.

[9] Further information is available in Definitions or on CAG webpages

[10] These alternative opt-out mechanisms are set out in section 7 for completeness.

5.3 Records containing information about multiple individuals

In some circumstances an individual's record may contain confidential patient information about another person (such as a mother and baby in the same record).

The national data opt-opt applies to the entire record irrespective of whether an opt-out is identified for the individual who is the subject of the record (i.e. whom the record primarily relates to) or for a 3rd party whose confidential patient information is contained within the record.

However, it is recognised that the national data opt-out can only be applied in these circumstances where the NHS number is present for the third party. If the record only includes name or another identifier then it is not possible to apply the national data opt-out.

6 When does a national data opt-out not apply?

The following are exemptions from the national data opt-out:

6.1 Consent

The national data opt-out does not apply where explicit consent has been obtained from the patient for the specific purpose.

The application of the national data opt-out when researchers are seeking to contact a cohort of patients to ask their consent (so called consent for consent) is detailed in Section 7 - Consent for consent.

6.2 Communicable diseases 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 (Control of Patient Information) Regulations 2002 provides the lawful basis for the common law duty of confidentiality to be lifted. Public Health England oversees the use of this legal gateway on behalf of the Secretary of State for Health and Social Care.

Regulation 3 allows confidential patient information to be lawfully processed with a view to:

- 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
    - incidents of exposure to communicable disease
    - the delivery, efficacy and safety of immunisation programmes
    - 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.

6.3 Overriding 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.

This should be as a result of a positive public interest test having regard to the circumstances of the case. Data controllers are expected to have their own arrangements in place to apply the public interest test as and where necessary.

Examples of disclosures which may be made in the public interest include:

- 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

Further information and guidance about public interest is available on the Information Governance Alliance (IGA) website.

6.4 Information required by law or court order

The national data opt-out does not apply to the disclosure of confidential patient information where the information is required by law or a court order.

Examples of disclosures required by law are summarised below.

- the Care Quality Commission, which has powers of inspection and entry to require documents, information and records – a code of practice sets out how the CQC can use these powers (Health and Social Care Act 2008);
- NHS Digital when using its section 259 powers to collect information when directed by the Secretary of State or NHS England (Health and Social Care Act 2012);
- the NHS Counter Fraud Service, which has powers to prevent, detect and prosecute fraud in the NHS (National Health Service Act 2006);
- investigations by regulators of professionals (e.g. Health and Care Professions Council, General Medical Council, or Nursing and Midwifery Council investigating a registered professional's fitness to practise) (e.g. under the Medical Act 1983);
- coroners' investigations into the circumstances of a death, that is if the death occurred in a violent manner or in custody (Coroners and Justice Act 2009);
- health professionals must report notifiable diseases, including food poisoning (The Public Health (Control of Disease) Act 1984 and the Health Protection (Notification) Regulations 2010);
- the Chief Medical Officer must be notified of termination of pregnancy, giving a reference number, date of the birth and postcode of the woman concerned (Abortion Regulations 1991);
- employers must report deaths, major injuries and accidents to the Health and Safety Executive (Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013);
- information must be provided to the police when requested to help identify a driver alleged to have committed a traffic offence (The Road Traffic Act 1988);
- information must be provided to the police to help prevent an act of terrorism or prosecuting a terrorist (The Terrorism Act 2000 and Terrorism Prevention and Investigation Measures Act 2011);
- information must be shared for child or vulnerable adult safeguarding purposes (e.g. s.47 Children Act 1989);
- health professionals must report known cases of female genital mutilation to police (Female Genital Mutilation Act 2003)
- judge or presiding officer of a civil or criminal court can require disclosure of confidential patient information through a court order
- information required to be reported to HFEA for inclusion on the register of assisted reproduction and fertility treatments (Human Fertilisation and Embryology Act 1990
- some disclosures of information to ONS (please see Data flows to ONS for official statistics for further information of the impact of the national data opt-out on such disclosures)
- disclosure of information relating to transplant approvals and serious and adverse reactions notifications (Human Tissue Act 2004)
- responsible bodies including health boards, trusts and regulatory bodies are required to co-operate on the handling of, and acting on, shared information relating to the management and use of controlled drugs. (The Controlled Drugs (Supervision of Management and Use) Regulations 2013)

This is not an exhaustive list, so information governance and/or legal advice should be sought where necessary. Further details are available in Appendix 5: Information required by law or court order.

It should be emphasised that any legal requirement must set aside the common law duty of confidentiality. It should be noted that the exercise of a statutory function does not necessarily constitute a legal requirement for the disclosure of confidential patient information – organisations should always give due regard to the common law duty of confidentiality.

7 Policy considerations for specific organisations or purposes

7.1 Payments and invoice validation

In general the national data opt-out does not apply to data used for payment and invoice validation purposes. Specifically the national data opt-out does not apply to invoice validation for non-contracted activities and for contracted activity anonymised data should be used.

Recognising the financial risks, the NDG review set out a clear position on the use of confidential patient information for invoice validation for non-contracted activity (non-contracted activity refers to services delivered by a health or care provider, where there is no agreed contract with the patient's responsible commissioner. For example, a patient may live in Bromley and be taken critically ill whilst on holiday in Devon. South Devon and Torbay CCG will send an invoice to Bromley CCG for the patient's care. Bromley CCG will want to check that they are responsible for the patient before paying the invoice).

The review states *"Taking into account the importance of accurately allocating NHS resources and the lack of evidence of public concern in relation to the use of data for this specific purpose, it is recommended that invoice validation for non-contracted activity should be an exception to the opt-out"***.**

The following policy statements apply to data processing in support of payments and invoice validation:

- Unless there is no alternative, data flows for payments and invoice validation should not use identifiable data - in particular - where a contractual relation exists between the commissioner and provider. In such cases anonymised data can almost certainly be used and national data opt-outs **do not** apply - provided data is anonymised in line with the ICO Code of Practice on Anonymisation.
- National data opt-outs **do not** apply where a patient has given their explicit consent for the use of their data for payment and invoice validation. All organisations within health and adult social care should be as transparent as possible as to how confidential patient information is being disclosed for payment purposes in order to better manage patient expectations.
- National data opt-outs **do not** apply to data disclosed for the purpose of non-contracted invoice validation
- National data opt-outs **do** apply to data disclosure for payment purposes which rely on S.251 support unless the standard condition requiring patient opt-outs to be respected is waived or it relates to non-contracted activity. However, national data opt-outs **do not apply under the specific conditions** of the following approvals as CAG have waived the standard condition:
    - Application for transfer of data from the HSCIC to commissioning organisation accredited safe havens: inclusion of invoice validation as a purpose within CAG 2-03 (a)/2013 (CAG 7-07(a)/2013)
    - Invoice validation within Clinical Commissioning Groups (CCGs) controlled environment for Finance (CAG 7-07(b)/2013)
    - Invoice validation within NHS England within the Commissioning Support Units controlled environment for Finance on behalf of Clinical Commissioning Groups (CAG 7-07(c)/2013)
- National 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

the National Health Service (Pharmaceutical Services, Charges and Prescribing) (Amendment) Regulations 2018[11].

7.2 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 S.251 of the NHS Act 2006 is relied upon to support the disclosure.

The NDG review considered risk stratification for case finding and risk stratification for planning as two separate functions. The Review goes on to state that: *"risk stratification for case finding, where carried out by a provider involved in an individual's care or by a data processor acting under contract with such a provider, should be treated as direct care for the purpose of the opt out (and therefore should not be subject to the opt out of personal confidential data being used for purposes beyond direct care)".*

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[12], 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 S.251 support unless the standard condition requiring patient opt-outs to be respected is waived [13].

7.3 Cross border data flows

National data opt-outs apply where confidential patient information about an individual's health and adult social care provided in England is disclosed outside of England in line with the wider policy.

This includes information disclosed to home nations, that is Wales, Scotland, Northern Ireland, the Isle of Man or Channel Islands but also other countries, for example where data is disclosed with S.251 support for research purposes.

7.4 Consent for consent

Where researchers need to identify people to participate in research studies, the national data opt-out may apply to this process depending on the mechanism used to identify potential research subjects.

In certain scenarios, researchers may need to access confidential patient information to identify people with particular conditions or characteristics to invite them to take part in clinical trials and other interventional studies. This process is often referred to as seeking "consent for consent". There are a number of established mechanisms for identifying potential research subjects which are set-out in the 2013 IG Review and the application of the national data opt-out to each of these is summarised below:

---

[11] https://www.legislation.gov.uk/uksi/2018/1114/regulation/15/made

[12] or by a data processor acting under contract with such a provider.

[13] The assumption being that if section 251 approval is required, this could not be considered as an individual (or direct) care purpose

Mechanism for identifying the cohort for a research study	National data opt-out applies?
The researcher gains the explicit consent of every patient with a record in the population pool being assessed	No
The search is conducted by a health or social care professional who has a "legitimate relationship" with the patient, such as a clinician or social worker	No
The search is conducted by a researcher who is part of the immediate clinical team	No
The search makes use of "privacy enhancing technologies"[14]	No
Support under Section 251 regulations is granted for the research to contact suitable patients to seek their consent	Yes

7.5 Flows to Public Health England National Disease Registers

The national data opt-out does not apply to confidential patient information flowing to Public Health England (PHE) under the following approvals:

i. **National Cancer Register (PIAG 03(a)/2001);**

ii. **National Congenital Anomaly and Rare Diseases Register (CAG 10-02(d)/2015).**

These national disease registers continue to operate separate opt-out mechanisms. For further information, see the National Cancer Registration and Analysis Service and National Congenital Anomaly and Rare Disease Registration Service websites. Data should continue to flow to PHE in full under these approvals as these specific opt-outs are registered directly with PHE and are applied by PHE on landing.

In addition to the specific national disease register opt-outs PHE also applies national data opt-outs to its onward releases of data from the national disease registers to other organisations in line with the national data opt-out policy.

7.6 Data flows to ONS for official statistics

The national data opt-out does not apply to data flowing into the Office for National Statistics (ONS) solely for the production of official statistics.

The NDG review recognised the importance of maintaining the integrity of official statistics and for this reason it did not make "*data flows into the ONS for the production of official statistics part of the proposed opt-out*".

The ONS has a range of legal gateways that it can use to access data for statistical purposes under the Statistics and Registration Service Act 2007, as amended by the Digital

[14] Analytical computer software that can trawl clinical databases, selecting only those patients who are eligible for a specific study, and only reveal the identities of potential participants to someone with a legitimate relationship to the patient, such as their clinician or social worker.

Economy Act 2017. The national data opt-out does not apply to data accessed by ONS for the production of official statistics, specifically:

- National data opt-outs **do not** apply to confidential patient information flowing into ONS under section 45A – section 45C of the Statistics and Registration Service Act 2007 (as inserted by the Digital Economy Act 2017) for the production of official statistics.
- National data opt-outs **do not** apply to patient registration information disclosed to ONS under section 43 of the Statistics and Registration Service Act 2007 because this is not confidential patient information.

The application of the national data opt-out to any disclosures of confidential patient information to the ONS for any other purposes (for example, research) and which are not for the production of official statistics will be considered in line with this policy, taking into account the legal basis for the data flow.

7.7 Population screening programmes

The national data opt-out does not apply to disclosures of confidential patient information for the purpose of allowing participation in National Screening Programmes endorsed by the UK National Screening Committee.

The NDG review took a specific position on population screening programmes: *"Some uses of information for public health purposes can be seen as direct care, that is where they relate to the care of an individual. This includes the oversight and provision of population screening programmes"*.

For the avoidance of doubt national data opt-outs **do not** apply to confidential patient information flowing under the following approvals:

i. NHS Breast, Bowel and Cervical Cancer Screening Programmes (15/CAG/0207);
ii. NHS Abdominal Aortic Aneurysm Screening Programme (ECC 3-04(o)/2011).

These screening programmes continue to operate separate opt-out mechanisms for patients who do not wish to be invited for screening.

Public Health England (PHE) is responsible for the national coordination and quality assurance of the population screening programmes.

PHE applies national data opt-outs to its onward releases of data from the national screening programmes to other organisations in line with the national data opt-out policy.

7.8 Assuring Transformation

The national data opt-out does not apply to confidential patient information about people with learning disabilities and/or autism who are in hospital for their mental health or due to challenging behaviour which is disclosed under the following approval:

- **Assuring Transformation: Enhanced Quality Assurance Process Data flow (CAG 8-02 (a-c)/2014).**

These flows continue to operate a separate opt-out mechanism and details of how to opt-out of the Assuring Transformation data collection can be found on the NHS England webpages. This exemption is time limited until the end of the "Building the Right Support Programme".

7.9 National patient experience surveys

The national data opt-out does not apply to the National Cancer Patient Experience Survey (CPES) and CQC NHS Patient Survey Programme, both of which will continue to run unaffected[15] under their current arrangements.

These national surveys will continue to operate separate opt-out mechanisms and details of how to opt out of these surveys are provided locally by the organisations undertaking the surveys e.g. posters in A&E for opting out of the A&E survey.

7.10 NHS Digital

The policy for the application of national data opt-outs to data flows into and out of NHS Digital (formerly known as the Health and Social Care Information Centre (HSCIC)) is as follows. It should be noted that these recognise NHS Digital's role as the national safe haven and the specific powers it has under the Health and Social Care Act 2012:

7.10.1 Data flows into NHS Digital

National data opt-outs do not apply to flows of data into NHS Digital where these are required under s259 of the Health and Social Care Act 2012 following a Direction from Secretary of State or NHS England or a mandatory request.

This was supported by the NDG Review:

"The Review proposes that personal confidential data should be passed to the HSCIC, as the statutory safe haven of the health and social care system, to de-identify or anonymise and share it with those that need to use it. If HSCIC were able to disseminate high quality anonymised data based on a complete dataset, it would reduce the need for these organisations to access personal confidential data. For that reason the Review recommends that, in due course, the opt-out should not apply to any flows of information into the HSCIC".

NB: There may be some instances where flows of data into NHS Digital will be subject to the national data opt-out, for example where NHS Digital are acting as a data processor on behalf of another organisation and the legal basis for the disclosure is support under S.251.

7.10.2 Disclosures by NHS Digital

National data opt-outs do apply to disclosures of confidential patient information by NHS Digital in line with this policy.

7.10.3 Return of data to submitting organisation

National data opt-outs do not apply to data disclosed by NHS Digital in accordance with section 261(4) of the 2012 Act where NHS Digital is disclosing confidential patient information to the organisation from whom NHS Digital originally collected the confidential patient information.

Specifically, this covers data returned to the submitting organisation providing no additional confidential information is supplied. For example, the return of Secondary Uses Service (SUS) data to providers. Additional information which is not confidential and which the submitting organisation would be permitted to receive includes items derived or calculated from the submitted information such as age or CCG of residence.

In all other circumstances national data opt-outs do apply unless otherwise exempt in line with this policy.

[15] Subject to S251 and other relevant approvals

7.10.4 Open data and publications

National data opt-outs do not apply to open data or statistics published by NHS Digital where this is subject to disclosure controls and is fit for publication.

Such data is deemed to be anonymous and individuals cannot be identified.

8 Applying the national data opt-out

Health and care organisations are required to apply national data opt-outs in line with this policy with all organisations achieving compliance by March 2020.

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 this policy.

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 disclose[16]. 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. There is also a forthcoming Information Standard on Compliance with the National Data Opt-out which will set out the requirements to achieve compliance and signposts to further technical and implementation guidance.

The policy rules for applying national data opt-outs are set out below:

8.1 Record removal

Where a national data opt-out needs to be applied this means that the entire record, or records, associated with that individual must be fully removed from the extract or dataset used for this purpose. It is not permitted to simply remove identifiers or otherwise de-identify part of the record (such that the data is still not anonymised in line with the ICO Code of Practice) due to the risks of re-identification associated with this approach.

It should be noted that source, or underlying records, held in systems may still be needed, for example for individual care purposes, and the opt-out does not require such records to be removed. In most cases it is expected that datasets for purposes beyond individual care will be derived or extracted and the opt-out can then be applied without an impact on the source data.

If more than one file is to be released to another organisation without the opt-out having been upheld (as a result of the statements or exemptions in this policy) care must be taken to ensure that no common identifiers can be used to re-identify records of individuals.

For example, consider an organisation releasing multiple related files, the first of which is anonymised in line with the ICO Code of Practice and the second being data which is not confidential but contains patient identifiers. If an identifier appears in both datasets, this could be used to re-identify the individual.

[16] Organisations would still need to have the appropriate legal basis for any such disclosures. This must not be interpreted as, or confused with, a patient's explicit consent to the sharing of their data.

8.2 NHS number

Where a national data opt-out has been set, it is recorded against an individual's NHS number and the NHS number is used as the single identifier for applying the national data opt-out. The following policy lines apply to the use of NHS number for applying national data opt-outs:

- The NHS number is used as the single identifier to register and to apply an individual's national data opt-out. No other patient identifiers are used to identify patients and apply national data opt-outs.
- Organisations are not required to 'trace' NHS numbers specifically for the purpose of applying the national data opt-out outside of that required for existing good practice. That is in instances where the NHS number is missing or inaccurate within datasets or individual records. Where NHS numbers are easily attainable opt-outs should be applied as in the table below:

Scenario	Opt-out applies?
NHS number available within the data to be released	Yes
1)NHS number missing or inaccurate within the data to be released AND 2)The effort in obtaining the NHS number from other sources within the [flow/system/organisation] is not disproportionate to the number of missing or inaccurate records.	Yes
1)NHS number missing or inaccurate within the data to be released AND 2)The effort in obtaining the NHS number from other sources within the [flow/system/organisation] is disproportionate to the number of missing or inaccurate records. AND 3) Existing good practice about NHS number tracing and data quality has been adhered to.	No

- Organisations must not deliberately remove or omit the NHS number from data flows containing other confidential patient information in order to prevent the national data opt-out from being applied correctly in line with this policy.
- In some instances, patient identifiers including NHS number have been intentionally removed from records to prevent the individual from being identified, such as for patients with legally restricted conditions[17] or in line with a consent model. In these cases, no attempt should be made to re-identify the individual in order to apply the national data opt-out as this may be detrimental to the confidentiality and privacy of the individual and could breach legal restrictions.

[17] For example identifying individuals who have received IVF is restricted by the Human Fertilisation and Embryology Act 1990 as amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992

An Information Standard provides the specification for use of the NHS number by NHS bodies and by other organisations providing health and care services in England in partnership with the NHS. Section 251A of the Health and Social Care Act 2012[18], together with the regulations made under S.251A(1)[19], provide that the NHS number **must** be used by commissioners and providers as the consistent identifier when processing information about a patient for their direct care.

8.3 Timing of application of the national data opt-out

A national data opt-out is applied to confidential patient information at the point it is disclosed for purposes beyond individual care. The most up-to-date national data opt-out must be applied at this point.

A national data opt-out applies to all confidential patient information in relation to the individual in scope, including any historic patient records being disclosed for a specific purpose.

A national data opt-out does not apply retrospectively, meaning it does not need to be applied to data that has already been processed. At the point a particular dataset has been used or released, all patients who have opted out at that time should be removed. Data does not need to be recalled once released or otherwise processed.

A patient may choose to change their opt-out decision at any time and their current choice is respected at any given time, replacing any previous choices made. If a patient has previously opted out, but then subsequently withdraws their opt-out, their confidential patient information (including any historic data) will become available for use beyond their individual care once again. This is true even where the data relates to a period where the patient had previously opted out.

An individual is not able to set a preference that specifically applies to data over a defined period of time, although as described in the NDG Review they can choose to give explicit consent (under common law) for a particular use of their data. For example, a research project or clinical trial.

An organisation is expected to comply with the conditions set out in their data sharing agreements with regards to data retention/destruction and onward sharing of data for future uses. There is no specific requirement for an organisation to remove an individual's record from data they have already received as a result of an individual's opt-out preference being changed. However, data sharing agreements may include specific arrangements for the application of the most up-to-date national data opt-out prior to onward sharing if required by the data controller.

It is recommended that where the terms of the use of the data allow onward sharing that data controllers should consider, as good practice, adding such a condition which requires the most up to date national data opt-out list to be applied at this point.

8.4 Time lag for applying national data opt-outs

National data opt-outs may take up to 21 days from being registered with NHS Digital to being fully applied to all disclosures of data.

Patients setting a national data opt-out have been provided with clear information that it may take up to 21 days for their opt-out to be applied across all disclosures of data. The service to check for national data opt-outs is updated every 24 hrs which gives local organisations

[18] As amended by the Health and Social Care (Safety and Quality) Act 2015

[19] Health and Social Care Act 2012 (Consistent Identifier) Regulations 2015 (SI 2015/1439)

who access the service directly 20 days to process and disclose the data. Where a temporary cache of the data is held locally this must be updated at least every 7 days and in this case the organisation has 13 days to process and disclose the data.

8.5 Use of national data opt-out data by health and care organisations

Data received by organisations through the service to check for national data opt-outs is provided for the sole purpose of applying national data opt-outs in line with this policy.

In line with the information provided to patients setting a national data opt-out the cleaned list provided to organisations is to enable compliance with the national data opt-out policy. It must be stored securely and accessed on a need to know basis only. Specifically, it must not be:

- used to explicitly identify patients with a national data opt-out
- added to, or stored, on a patient record
- used to explicitly provide clinicians or other care staff with a view of a patient's national data opt-out preference other than where is this essential for the purpose of applying opt-outs. For example, it should not be used to consider an individual's suitability for research.

Further details on the use of the data received through the service to check for national data opt-outs will be included in the Information Standard on Compliance with the National Data Opt-out and in the licence [DN: Link to licence] for the use of this data.

9 Analysis of national data opt-outs

9.1 National data opt-out publication

A national data opt-out publication provides statistics on the volume and spread of national data opt-outs. The publication gives a breakdown of national data opt-outs against different demographic metrics including age, gender, GP practice, Clinical Commissioning Group (CCG) and Lower Layer Super Output Area (LLSOA). This is updated monthly.

9.2 Bespoke Analysis

Health and adult social care organisations may wish to undertake more bespoke or specific analysis to understand the potential impact of national data opt-outs on the data that they disclose or receive. Any analysis needs to meet the following principles:

- Undertaken in a way that prevents the identification of an individual with a national data opt-out, for example by comparing counts where opt-outs have and have not been applied. National data opt-outs must not be directly linked to other datasets.
- Dimensions analysed independently of each other/small number of dimensions combined to reduce risks of re-identification
- Resulting analysis must be fit for publication/anonymised in line with the ICO Code of Practice on Anonymisation

10 Compliance with the national data opt-out

The national data opt-out is a policy offering set by the DHSC and gives effect to the right set out in the NHS Constitution to *"request that your confidential information is not used beyond your own care and treatment"*. The policy is intended to implement the recommendations of the NDG review and thereby help to increase public confidence and trust in the use of their health and care data.

A number of mechanisms have been put in place to ensure that organisations within health and adult social care comply with the national data opt-out policy as required. Principally this is a combination of information standards, statutory guidance, contractual levers, legal requirements and information for the public to increase visibility and transparency of compliance at a local level.

It should be noted that health and adult social care bodies are legally required to "have regard to" information standards[20] and statutory guidance[21]. Whilst these are not an absolute legal obligation - an organisation that did not comply with an information standard or statutory guidance may be leaving themselves open to legal challenge.

10.1 Code of Practice on Confidential Information

Any organisation that collects, analyses, publishes or disseminates confidential health and care information is legally required to "have regard to" the NHS Digital Code of Practice on Confidential Information based on section 263 of the Health and Social Care Act 2012 (HSCA). The code of practice is published by NHS Digital and clearly defines the steps that organisations must, should and may take to ensure that confidential information is handled appropriately. This includes the application of national data opt-outs in line with this policy.

10.2 Data Security and Protection Toolkit

The Data Security and Protection (DSP) Toolkit (which replaced the Information Governance (IG) Toolkit) includes an evidence item on compliance with the national data opt-out[22]. This requires organisations to self-declare their compliance (or otherwise) with the policy and provide a clear public statement to this effect. It is of note that compliance may not require an organisation to actually apply national data opt-outs e.g. where an organisation only processes CPI for individual care. The DSP toolkit is an information standard.

10.3 Information standard on compliance with the national data opt-out

An information standard on compliance with the national data opt-out is in the process of being developed. This standard mandates organisations to comply with the national data opt-out policy and to use the technical service to check for national data opt-outs in line with technical specifications and instructions. It also specifies the compliance timeframe as part of the implementation guidance element of the standard.

10.4 Contracts

NHS contracts and those based on the NHS standard contract include a requirement to comply with all information standards. Failure to do so may be considered a breach of contract.

---

[20] made under Section 250 of the Health and Social Care Act 2012

[21] issued under Section 263 of the Health and Social Care Act 2012

[22] the wording for the evidence item is subject to confirmation in the 2019/20 version of the toolkit

10.5 Information Commissioner's Office (ICO) Position

Although the national data opt-out is a policy offer to allow patients some additional choice about how their confidential patient information is used the ICO have set out their position on how they may consider cases where the national data opt-out was not applied when it should have been. Specifically, failure to comply with the national data opt-out policy could be seen as a breach of the requirements for processing to be fair and transparent.

11 Further Information

11.1 Further information

For more information about the national data opt-out, how it works and to set a preference, please visit the national data opt-out service webpages.

For further information and support relating to this policy and information on the phased implementation of application of national data opt-outs across health and adult social care, please visit the national data opt-out programme webpages. These pages include a range of factsheets, guidance for health and care staff and resources for staff and patients.

11.2 Background information and reference documents

The following links provide background information and link to useful references:

National Data Guardian Review of data security, consent and opt outs

Government response to the National Data Guardian Review

Understanding Patient Data

Confidentiality Advisory Group pages

Confidentiality: NHS Code of Practice

IGA GDPR Guidance

11.3 Contact details

If you require further information that is not available from the links above, have any questions or would like to provide feedback on this document please contact the National Data Opt-out Programme via the following channels:

- Email: enquiries@nhsdigital.nhs.uk (please include 'national data opt-out policy' within the subject line)
- Telephone (Contact centre): 0300 303 5678

Appendix 1: Abbreviations

Term / Abbreviation	What it stands for
AQP	Any Qualified Provider
BSA	NHS Business Services Authority
CAG	Confidentiality Advisory Group
CCG	Clinical Commissioning Group
CLDC	Common law duty of confidentiality
CPI	Confidential Patient Information
CQC	Care Quality Commission
DHSC	Department of Health and Social Care (formerly Dept. of Health – DH)
DMS	Defence Medical Services
DSA	Data Sharing Agreement
DSPT	Data Security and Protection Toolkit
DWP	Department for Work and Pensions
FGM	Female Genital Mutilation
GDPR	General Data Protection Regulation
GP	General Practitioner
GRO	General Registrar's Office
HSCA	Health and Social Care Act (2012)
HSCIC	Health and Social Care Information Centre (now NHS Digital)
ICO	Information Commissioner's Office
IGA	Information Governance Alliance
NDG	National Data Guardian
NDOP	National Data Opt-out Programme
NHS	National Health Service
ONS	Office for National Statistics
PDF	Portable Document Format
PDS	Personal Demographic Service
PHE	Public Health England
PIT	Public Interest Test
SBS	NHS Shared Business Services
SRSA	Statistics and Registration Service Act 2007
SUS	Secondary Uses Service
XML	Extensible Mark-up Language

Appendix 2: Definitions

For the purpose of this policy the following definitions have been used.

A2.1: Individual or Direct Care

The following definition of individual (also called direct) care as set out in the NDG Review is used to underpin the national data opt-out

"A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care."

The NDG review gave some further clarity on local clinical audit as follows:

"The use of personal confidential data for local clinical audit is permissible within an organisation with the participation of a health and social care professional with a legitimate relationship to the patient through implied consent. For audit across organisations, the use of personal confidential data is permissible where there is approval under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002".

These policy definitions need to be considered in the context of the legal framework around sharing of a patient's data for direct care, including the need for a lawful basis to process the data under the data protection legislation. Under section 251B of the Health and Social Care Act 2012[23] all commissioners and providers of health and care are required to share a patient's data with other relevant commissioners or providers where 'it is likely to facilitate the provision to the individual' of health or care in England. This statutory duty is subject to the common law duty of confidence (CLDC), which will be complied with in circumstances where the patient knows or reasonably expects that their data will be shared in such circumstances, i.e. there is implied consent. Section 251B and implied consent under CLDC will together provide the lawful basis to share in most cases of direct care. In these cases, and any cases of direct care based on explicit consent, the national data opt-out will not apply.

For completeness the Information Governance Review also defined what should be considered indirect care or purposes beyond individual care to be:

"Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment, financial audit."

[23] As amended by the Health and Social Care (Safety and Quality) Act 2015

A2.2: Data Controller

In this guidance, 'data controller' has the same meaning as 'data controller' or 'controller' in the Data Protection Act 2018 and the GDPR. Article 4(7) GDPR defines 'controller' as follows:

"'controller' means 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 Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;"

A2.3: Data Processor

Again 'data processor' has the same meaning as 'data processor' or 'processor' in the Data Protection Act 2018 and GDPR. Article 4(8) GDPR defines 'processor' as follows:

"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"

A2.4: Section 251 (S.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"). These regulations enable the disclosure of confidential patient information without consent, and without there being a breach of the common law duty of confidentiality, as long as the requirements of the regulations are met. The person responsible for the information must still comply with all other relevant legal obligations including data protection legislation. 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.
- 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 HRA 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 i.e. the Health Research Authority for research applications and the Secretary of State for Health and Social Care for non-research applications. 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.

A2.5: Health and adult social care system

The term “health and adult social care system” in this document is defined in section 4.1 and refers to organisations and associated processes that are part of health and adult social care. It does not refer to a specific information technology (IT) system or set of IT systems.

A2.6: Patients, members of the public and service users

A number of different terms are used throughout health and adult social care to refer to the people for whom services are provided. In health, the term ‘patient’ is generally used while in adult social care, a variety of terms are used, including ‘service user’. However, a person setting an opt-out may not necessarily be either a ‘patient’ or a ‘service user’. For the purposes of this document, the term ‘member of the public’ and ‘person’ will be used to refer to an individual in the context of setting an opt-out and the term ‘patient’ will be used in the context of an organisation applying an opt-out.

A2.7: Setting and applying opt-outs

The term ‘setting’ in the context of national data opt-outs is used to refer to the processes whereby a member of the public uses one of the available channels to set a national data opt-out. The term ‘applying’ is used to refer to the processes whereby organisations within health and adult social care apply the national data opt-out to any data disclosures.

Appendix 3: Rationale and Supporting Information

This appendix further details the rationale and background to some of the policy statements in this document:

A3.1: Who can opt out

The following sections outline the rationale behind some of the policy approach on setting an opt-out:

A3.1.1: PDS record as the basis for being able to set an opt-out

The intention is that the national data opt-out should be available to anybody who has received care from the health and adult social care sector in England and, therefore, have data about them in the system. The intention is that as many patients as possible who fall into this category are able to set an opt-out. Therefore, the decision was taken that the opt-out should be available to everybody who has a record on PDS. This potentially includes patients who are not resident in England but may have received care from the health and adult social care sector in England.

A3.1.2: Formal proxy and opt-out setting

The decision was taken to allow formal proxies (individuals who have a formal, legal relationship to act on behalf of another) to set an opt-out by proxy. This is to allow as many people as possible to have an opt-out and not disadvantage key groups of people. In order to minimise any potential misuse of the system this has been restricted to someone who has formal legal powers to represent the other individual. For this reason, lasting powers of attorney (LPA) for both health and welfare and property and financial matters and court appointed deputies are able to act as a formal proxy.

A3.1.3: Minimum age to independently set an opt-out

There are a range of different ages at which children are expected to make decisions about their medical treatment and use and access to medical information. In some cases, where these decisions are made in a clinical setting, a health professional may be required to determine the competence of a child to make such a decision.

GDPR sets out specific requirements around privacy for Information Society Services - which has a specific definition and is normally for remuneration (this includes advertisement income). Online health services are likely to be outside this definition as they are not paid for services. But data protection law does set 13 as the age at which a child does not need parental consent for the processing of their personal data online, that is that they can consent themselves to such processing. The national data opt-out has aligned with this legal age and 13 has been set as the minimum age from which children can set their opt-out preference through any channel. The legal minimum age in data protection law is seen as the most directly applicable law or guidance for this policy decision. Below 13 an opt-out can be set by someone with parental responsibility. Any national data opt-out that has been set by a person with parental responsibility for a child under the age of 13 will remain in place after the child reaches the age of 13. This setting will only change if the child/young person proactively decides to change their national data opt-out setting when they reach the age of 13 or after that.

Appendix 4: Changes to NHS number

The National Back Office (NBO) provides a national data quality service and is responsible for the management of NHS numbers and Personal Demographics Service records.

A4.1: Duplicates and Confusions

In the event of duplications or confusions national data opt-outs will automatically be applied to the correct patient wherever possible. In the event that it is not possible to assign the opt-out to the correct patient automatically NHS Digital will write to the individuals affected.

For further information please see NHS Digital Data Quality Incidents.

A4.2: Assigning new NHS Numbers

In instances where individuals are allocated a new NHS number any existing national data opt-out will not automatically be transferred to the new record. This will include the following:

- Adoptions
- Gender reassignment
- Identity protection

Instead such individuals will receive a letter informing them of the national data opt-out to ensure that they understand their options either via NHS Digital or the individual who is handling their case.

Appendix 5: Information required by law or court order

Further details of examples of disclosures required by law are defined in the table below:

Area	Legal Requirement	URL
Care Quality Commission	the Care Quality Commission, which has powers of inspection and entry to require documents, information and records – a code of practice sets out how the CQC can use these powers	Health and Social Care Act 2008
NHS Digital (formerly HSCIC)	NHS Digital, the statutory safe-haven, which has powers to collect information when directed by the Secretary of State or NHS England	Health and Social Care Act 2012
NHS Counter Fraud	the NHS Counter Fraud Service, which has powers to prevent, detect and prosecute fraud in the NHS	Part 10 of the National Health Service Act 2006
Fitness to Practice Investigations	investigations by regulators of professionals (e.g. Health and Care Professions Council, General Medical Council, or Nursing and Midwifery Council investigating a registered professional's fitness to practise)	e.g. under section 35a of the Medical Act 1983
Coroners	coroners' investigations into the circumstances of a death. For example if the death occurred in a violent manner or in custody	Coroners and Justice Act 2009
Notifiable Diseases	health professionals must report notifiable diseases, including food poisoning	The Public Health (Control of Disease) Act 1984 Public Health (Infectious Diseases) Regulations 1988 Health Protection (Notification) Regulations 2010)

Area	Legal Requirement	URL
Termination of Pregnancy	the Chief Medical Officer must be notified of termination of pregnancy, giving a reference number, date of the birth and postcode of the woman concerned	Abortion Regulations 1991
Health and Safety	employers must report deaths, major injuries and accidents to the Health and Safety Executive	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
Road Traffic Offences	information must be provided to the police when requested to help identify a driver alleged to have committed a traffic offence	The Road Traffic Act 1988
Prevention of Terrorism	information must be provided to the police to help prevent an act of terrorism or prosecuting a terrorist	Section 38B of The Terrorism Act 2000 Terrorism Prevention and Investigation Measures Act 2011
Safeguarding	information must be shared for child or vulnerable adult safeguarding purposes Provision of information to safeguarding adult boards at its request to enable or assist the board to perform its functions.	e.g. s.47 Children Act 1989 Care Act 2014
Female Genital Mutilation (FGM)	health professionals must report known cases of female genital mutilation to police	Female Genital Mutilation Act 2003
Court Orders	Judge or presiding officer of a civil or criminal court can require disclosure of confidential patient information through a court order	

Area	Legal Requirement	URL
Human Fertilisation and Embryology Authority	Information required to be reported to HFEA for inclusion on the register of assisted reproduction and fertility treatments[24]	Human Fertilisation and Embryology Act 1990
ONS	Disclosure of information required to enable ONS to exercise one or more of its functions[25]	Statistics and Registration Act 2007 (as amended by the Digital Economy Act 2017)
NHS Resolution Litigation	Disclosure of information for investigating and defending legal claims	Section 35 Data Protection Act 1998
Human Tissue Authority	Disclose of information relating to transplant approvals and serious and adverse reactions notifications.	Human Tissue Act 2004 HTA Guidance
Controlled Drugs	Responsible bodies including health boards, trusts and regulatory bodies are required to cooperate on the handling of, and acting on, shared information relating to the management and use of controlled drugs. Should usually be anonymised or with consent but in some instances may allow disclosure of confidential information	The Controlled Drugs (Supervision of Management and Use) Regulations 2013

[24] Legal restrictions also exist on the disclosure of human fertilisation and embryology information

[25] Only applies to information required by ONS – typically for the creation of official statistics

Appendix 6: Confidential Patient Information (CPI) definition

The national data opt-out applies to Confidential Patient Information (CPI) when it is disclosed for purposes beyond an individual's care and treatment. This appendix provides guidance for health and care professionals in assessing what is CPI for the purposes of applying the national data opt-out.

A6.1: What is Confidential Patient Information?

Confidential Patient Information is a legal term in use across the health and care system. It is defined in section 251[26] (11) of the National Health Service Act 2006 (see below). Broadly it is information about either a living or deceased person that meets the following 3 requirements:

a) identifiable or likely identifiable e.g. 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 definition of "patient" specifically includes an individual who needs or receives local authority social care or whose need for such care is being assessed by a local authority. Confidential Patient Information cannot be defined by a specific data item (e.g. name or postcode) alone, as it needs to be considered more broadly to take account the nature of the information and the circumstances of the record, including the reasonable expectations of a patient.

Prior to making a disclosure or using data for a purpose beyond individual care an assessment must be made that considers whether the information concerned is Confidential Patient Information; what the lawful basis is for the disclosure or change of purpose; and, if lawful, whether the national data opt-out needs to be applied in line with this operational policy guidance document. This guidance aims to provide information that will support this assessment and provide some illustrative scenarios that set out some of the relevant factors to consider in making this assessment.

It is important to remember that any personal data which is identifiable but is not deemed to be Confidential Patient Information (for example because it does not tell you anything about the health or care or treatment of the individual) still needs to be processed lawfully, fairly and transparently in line with wider data protection legislation.

Broadly there are 2 types of patient identifiable data held in the NHS:

- **patient registration data** – this is personal[27] data provided by the patient when they register for health services. Most often through a GP (for example through completing a GMS 1 form and/or through other local processes). Registration data comprises demographic data (for example name, address, NHS number etc) which uniquely identifies an individual but does not include any clinical or medical information. This enables the Secretary of State to maintain a list of patients in order to fulfil his

[26] Section 251 has been updated to ensure that the definitions used expressly include local authority social care (that is care provided for, or arranged by, a local authority).

[27] Patient registration data is classified as personal data under GDPR/Data Protection legislation

statutory duty to provide general medical services to the resident population of England. This registration data is collected and held separately to records of health, care or treatment in various clinical or care records. Registration data are used for a range of administrative purposes within the health and care system for example to facilitate transfer of medical records, to manage GP lists, enable payment of GPs, fraud prevention and to secure and allocate resources. The separation from clinical care records can be illustrated by the fact that it is possible to be registered as a patient before any clinical record is created for example through the visa application processes for overseas visitors.

- **Clinical/Care records** – this includes demographic information that identifies an individual alongside a range of information about their physical or mental health, their condition(s) and diagnoses, assessment of an individual's needs for social care services, records of care or treatment given that are gathered in from a range of health and care settings. Any identifiable information taken from your clinical/care records is always Confidential Patient Information. An individual may have a number of clinical/care records in a number of different settings for example dental records, GP records, hospital records. Registration data may be used to populate or update a clinical/care record.

The interactions of these two types of data are illustrated below:

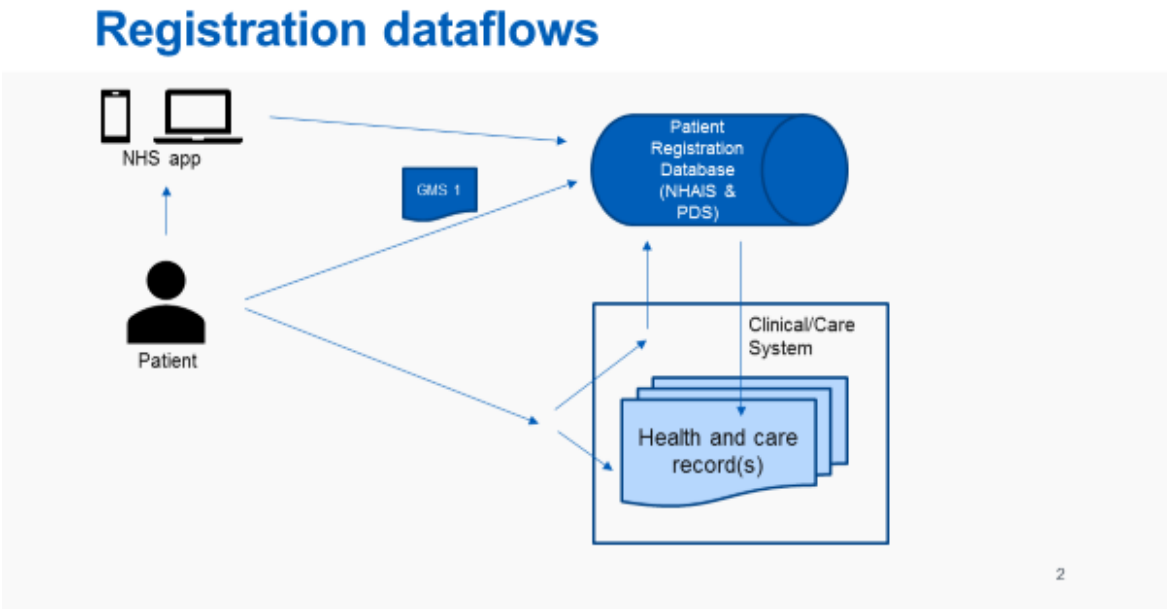

Figure 2: Registration dataflows

It is important that there is a complete list of patients for the NHS and care services and it is not possible to opt-out from the central patient register held on PDS. There are strict controls in place for use and access to patient registration data as this remains personal data.

It should be noted that in some circumstances clinical systems may be used to provide updates to patient registration data, for example where a patient has provided an update to their address during a clinical interaction. Such processes are for efficiency and convenience and in the future it is anticipated that patients will be provided with other mechanisms to enable them to provide such updates more directly (for example via an NHS app). The fact that the patient has provided an update to their address via a clinical

interaction does not mean that the information is owed a duty of confidence. The information provided must have the necessary 'quality' of confidence to be confidential, i.e. more than just a name and address. Separately there has to be a context (for example, confidential relationship, e.g. doctor/ patient) set by a patient's reasonable expectations that makes the information confidential. Most often such updates are provided to a receptionist.

A6.2: Assessing what is Confidential Patient Information

As set out above Confidential Patient Information cannot simply be defined by a specific data item (for example name or postcode) alone, as it needs to be considered more broadly to take account of the circumstances of the record and disclosure. There may be some other information provided at the time, or which can be inferred from the context of the disclosure, that means that it becomes Confidential Patient Information. This assessment needs to take into account what patients might reasonably expect to happen to their data in the particular circumstances in question and whether they might reasonably expect the national data opt-out to apply based on the information provided to them. The national data opt-out patient facing information and resources are found on the national data opt-out programme webpages – this, and other relevant patient information and communications, should be considered when making the assessment.

The national data opt-out public communication materials make it clear that the national data opt-out is limited to Confidential Patient Information and that patients cannot opt out of registration data. In addition the privacy notice for the Personal Demographic Service (the nationally held patient register) is also clear in this regard.

The following examples illustrate the factors that need to be taken into account when making this assessment particularly when considering demographic information in different scenarios:

Type of data and context of disclosure	Is it CPI	Rationale
Name and date of birth on its own drawn from registration data	No	Anyone can register to receive medical services whatever their state of health. This is identifiable, but it does not reveal anything about an individual's health, care or treatment.
Sample of NHS numbers drawn from registration data	No	NHS number on its own is not Confidential Patient Information – it is an administrative number assigned by the NHS. However, for someone with access to other NHS data it can act as the key to identify an individual. It is for that reason that it is protected by safeguards.

Type of data and context of disclosure	Is it CPI	Rationale
Name and address drawn from registration data	No	As for NHS number, name and date of birth, this is not Confidential Patient Information. However, connecting this identifying data to other information may make it Confidential Patient Information. For example for a very small number of patients who have no other correspondence address and where the address is an in-patient setting for people with severe learning disabilities or a specialist nursing home that cares for those with dementia then it may become Confidential Patient Information. This would be the case where the address itself said something about the individual's health, care or treatment.
Name and address – drawn from clinical records for example of those with a specific condition in order to write to them about a research study.	Yes	Although the disclosure is on the surface of it is demographic only - the circumstances of the disclosure may reveal something about a person's health, care or treatment if this is shared with a third party. However, where a clinician involved in the patient's care has written directly to the patient there is no disclosure of Confidential Patient Information and the opt-out would not apply.
Name and address drawn for a Patient Administration System (PAS) in a Mental Health Trust	Yes	The information is disclosed by a mental health trust and would constitute Confidential Patient Information as it does give some information about a person's health, care or treatment especially if it discloses that the person has either registered with the Mental Health Trust or has been treated.

A6.3: Further Information and Advice

The Information Governance Alliance has published a range of information and guidance on data protection and confidentiality for the health and care system.

The Confidentiality Advisory Group (CAG) is an independent body which provides expert advice on the use of confidential patient information. This includes providing advice to the Health Research Authority (HRA) and Secretary of State for Health and Care on the appropriate use of confidential patient information for purposes beyond individual patient care. As part of this CAG give advice about what constitutes Confidential Patient Information.

The Department of Health and Social Care has published a Code of Practice on Confidentiality[28]

NHS Digital has published a Code of Practice on Confidential Information[29]

A6.4: Extract from NHS Act 2006 Sec 251

The following is an extract from the NHS Act 2006 Sec 251 defining Confidential Patient Information:

(10) In this section "patient information" means—

(a) information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of his condition or to his care or treatment, and

(b) information (however recorded) which is to any extent derived, directly or indirectly, from such information,

whether or not the identity of the individual in question is ascertainable from the information.

(11) For the purposes of this section, patient information is "confidential patient information" where—

(a) the identity of the individual in question is ascertainable—

(i) from that information, or

(ii) from that information and other information which is in the possession of, or is likely to come into the possession of, the person processing that information, and

(b) that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual.

NB: It is worth noting that Section 251 was recently updated to ensure that the definitions of 'patient information', 'confidential patient information' and 'medical purposes' expressly includes 'local authority social care'. The definition of "patient" now specifically includes an individual who needs or receives local authority social care or whose need for such care is being assessed by a local authority. All references to "care" within this definition now includes "local authority social care" which is defined as:

- social care provided or arranged for by a local authority, and
- any other social care all or part of the cost of which is paid for with funds provided by a local authority;

[28] This Code is being reviewed and is due to be updated

[29] This Code is being reviewed and is due to be updated

Appendix 7: External review of the national data opt-out policy

This guidance document underwent an external review process which involved organisations from across the health and social care sector. The table below lists the health and adult social care organisations who participated in the external review process for this guidance, and/or were involved in reviewing individual policy position papers and informing individual policy decisions.

Health and Adult Social Care Organisations involved in the review of the National Data Opt-Out Operational Policy Document

• Department of Health and Social Care • NHS England • National Data Guardian Panel and Steering Group • NHS Health Research Authority • Confidentiality Advisory Group • Office for National Statistics • Information Governance Alliance • Royal College of Physicians • Royal College of General Practitioners • Royal College of Nursing • NHS Business Services Authority • Local Government Association • Professional Records Standards Body • Public Health England • Healthcare Quality Improvement Partnership • NHS Blood and Transplant • Human Tissue Authority • Care Quality Commission • Clinical Practice Research Datalink • NHS Improvement • NHS Resolution • Healthwatch England • Wellcome Trust • National Association for Patient Participation • Association of Medical Research Charities • Macmillan Cancer • Care Provider Alliance • Genetics Alliance UK • Cancer Research UK • Richmond Group • Skills for Care • Association of Directors of Adult Social Services • Borough of Poole - Commissioning and Improvement – Peoples Services • City of Wolverhampton Council • Haringey Metropolitan Council • Kirklees Metropolitan Council • Lincoln County Council • York City Council • North Cumbria CCG • Cumbria Partnership NHS Foundation Trust	• Leeds Community Healthcare NHS Trust • Newcastle Upon Tyne Hospitals NHS Foundation Trust • Manchester University NHS Foundation Trust • East London Health Trust • Calderdale and Huddersfield NHS Foundation Trust • West London Mental Health Trust • Buckinghamshire Healthcare NHS Trust • East London NHS Foundation Trust • Leeds and York Partnership NHS Foundation Trust • South Essex NHS Foundation Trust • Medway NHS Foundation Trust • Spencer Private Hospital • University College London - Great Ormond Street Institute of Child Health Developmental Biology & Cancer Programme • University of Sheffield Advanced Manufacturing Centre • NHS Darlington Community Commissioning Group • Bristol, North Somerset and Gloucester Clinical Commissioning Group • North East Commissioning Support Unit (CSU) • NHS Arden & Greater East Midlands CSU • NHS North of England CSU • NHS South, Central and West CSU • NHS Midlands and Lancashire CSU • NHS South and West CSU • Leeds City Council • South Gloucester Council • NHS National Services Scotland • NHS Wales Informatics Service • Welsh Government • Scottish Government • Care England • National Care Forum • Tameside Metropolitan Borough Council • Mid Cheshire Hospitals NHS Foundation Trust • Queen Victoria Hospital NHS Foundation Trust