NHS
Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: SOP18
Issue number: 1.1

National Data Opt-Out

Lead executive	Medical Director
Authors details	Trust Records & Information Governance Manager 01244 397384

Type of document	Standard Operating Procedure
Target audience	All CWP staff
Document purpose	To provide staff with guidance to ensure that the Trust complies with the national data opt-out policy.

Approving meeting	Information Governance & Data Protection Sub-Committee	Date 16-Mar-20
Implementation date	31-Mar-20	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
IM7	Confidentiality policy
IM6	Information sharing policy

Document change history	
What is different?	Recoded in line with policy library reshape
Appendices / electronic forms	N/A
What is the impact of change?	N/A

Training requirements	Yes - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	N/A

Financial resource implications	None

External references

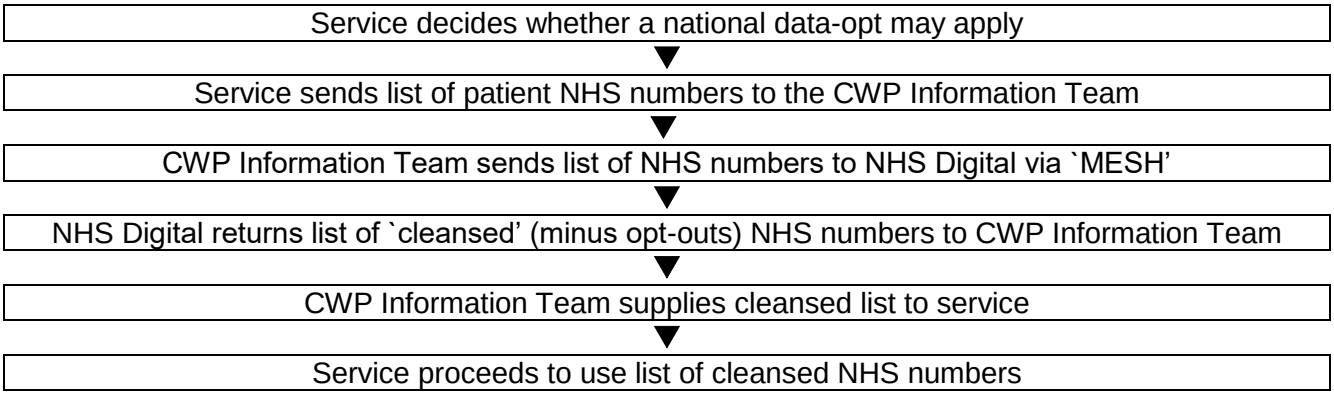
Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable? N/A		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	N/A	
What is the level of impact?	N/A	

Content

Quick reference flowchart for national data opt-out procedure

For quick reference the guide below is a summary of actions required.



1. Introduction

This standard operating procedure is to provide staff with guidance to ensure that the Trust complies with the national data opt-out policy.

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:

"The Review was persuaded that the best balance between meeting these expectations and providing a choice to those who have concerns is achieved by providing an opt-out model. The review concluded that people should be made aware of the use of their data and the benefits; an opt-out model allows data to be used whilst allowing those who have concerns to opt out".
The review also acknowledged that *"Whilst patients have a right under the NHS Constitution to request that their personal confidential data is not used beyond their direct care, there is currently no easy way for them to do that".*

The national data opt-out provides a single central mechanism which gives effect to this right.
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.

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* to health data used for direct care or 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.

2. Scope

This procedure is applicable to all staff, including contractors, temporary / agency staff and volunteers that are involved with disclosure of information.

2.1 Format of data

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.

2.2 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 and those individuals 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.

2.3 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.

2.4 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.

2.5 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.

3. When the national data opt-out applies

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 Common Law Duty of Confidentiality, 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.

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);
• 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 Section 251 of the NHS Act 2006

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 duty of 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

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 purposes3 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. 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 support Support under the Control of Patient Information Regulations Regulation 2 – for diagnosis and treatment of cancer or Regulation 5 – for the medical purposes set out in the schedule	Yes – in general **BUT** there are some specific exemptions	Data disclosure has Section 251 support obtained under regulation 2 or 5 of the Control of Patient Information Regulations. This applies unless the *Confidentiality Advisory Group (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.
Control of Patient Information Regulations 2002 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.

The national data opt-out does not apply where a patient has given their explicit consent to a 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 for that specific purpose.**

3.1 Disclosures using S.251 support – Health Service (Control of Patient Information)

Regulations 2002 Regulations 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 'the wishes of patients who have withheld or withdrawn their consent are respected' (e.g. their opt out). 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 S.251 applications each year, the CAG Registers give details of its approvals under S.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.

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. However, CAG reserves 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 Section 251 support (i.e. approval under the NHS (Control of Patient Information Regulations) 2002 (regulation 2 or 5)) 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.

3.2 Purpose and point of application

The national data opt-out applies to disclosures of data for purposes beyond individual care. More specifically:

• The national data opt-out would **always** need to be considered to be applied 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.

3.3 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. o 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)
o coroners' reports (coroners fall under the remit of Home Office)
o health assessment carried out by the Courts/legal service
o Her Majesty's Revenue & Customs
o health assessments undertaken privately for pension providers or insurance companies8
o universities, and
o Office for National Statistics (ONS) / General Registrar's Office (GRO)
o occupational health assessments

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 if the legal basis for the data disclosure is 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 using section 251 support.

4. When the national data opt-out does not apply

Consent

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

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:

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"	No
Support under Section 251 regulations is granted for the research to contact suitable patients to seek their consent	**Yes**

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.

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.

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.

Payments and invoice validation
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 such cases anonymised data can almost certainly be used and national data opt-outs **would 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.
• In accordance with the recommendations made in the NDG review, national data opt-outs **do not** apply to data disclosed for the purpose of non-contracted invoice validation (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 e.g. a patient receiving treatment in area that is outside of the CCG area where they are registered).
• 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 201811.
• National data opt-outs **only** 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.

Note: NHS England have a S.251 approval (CAG 7-07(a-c)/2013) in place covering data flows for invoice validation to Controlled Environments for Finance within CCGs and Commissioning Support Units.

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 care12, 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 **only** apply to data disclosures for risk stratification which rely on S.251 support unless the CAG approval letter states that the national data opt-out should not apply

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

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).

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.

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.

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).

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 unaffected15 under their current arrangements.

Data flows into NHS Digital
National data opt-outs do not apply to flows of data into NHS Digital (NHS Digital is the operating name for the Health and Social Care Information Centre (HSCIC)) where these are required under S.259 of the Health and Social Care Act 2012 following a Direction from Secretary of State or NHS England or a mandatory request.

Disclosures by NHS Digital
National data opt-outs do apply to disclosures of confidential patient information by NHS Digital.

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 Health and Social Care Act 2012 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.

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.

5. Process for applying the national data opt-out

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

NHS Digital has developed a technical service (MESH) 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.

Organisations can submit a list of NHS numbers that they need to disclose to NHS digital 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.

If you have worked out that the national data opt-out applies to your change of use or disclosure of data, you need to apply national data opt-outs by removing the records of anyone who has an opt-out registered before you use or disclose the information.

This is done by submitting a list of NHS numbers of those whose data is intended to be processed, to the CWP Information Team who will submit the list to NHS Digital who will cross-reference them against the central repository of national data opt-outs. NHS Digital will return a “cleaned list” to the CWP Information Team 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.

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.

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.

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 which rely on S.251 support. 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.

Where the terms of the use of the data (I.e. the specific S.251 approval) covers onward sharing, data controllers should apply the most up to date national data opt-out at this point. For example, an organisation that falls within the definition of health and care organisations set out in Section 4 may receive data from a health and social care provider under S.251 support and the S.251 support also allows this data to be linked with Hospital Episode Statistics (HES) data from NHS Digital. The national data opt-out would be applied at the point that the original data is disclosed from the health and social care provider to the organisation but it should also be applied at the point of disclosure to NHS Digital and also by NHS Digital when the linked data is returned to the research organisation.

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 will be 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 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.

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 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 this is essential for the purpose of applying opt-outs. For example, it should not be used to consider an individual's suitability for research.

6. Duties

6.1 Responsibilities

6.1.1 Chief Executive
The Chief Executive will assume overall accountability for ensuring that the Trust is compliant with the national data opt-out..

6.1.2 Trust Board
The responsibility for the provision of a national data opt-out procedure rests initially with the Trust Board and is delegated to the Information Governance Team. Additionally, the Trust Board will ensure

through the line management structures that this policy is applied and that staff are aware of the national data opt-out requirements.

6.1.3 Senior Information Risk Owner (SIRO)

The SIRO has ownership of the organisation's information risk policy and acts as advocate for information risk on the Board. The National Data Opt-Out Standard Operating Procedure (SOP) forms part of the Trusts overall Information Risk Framework. The SIRO is responsible for ensuring that the SOP is developed and implemented and that it is reviewed regularly to ensure that it remains fit for purpose and supports the Trusts compliance with Data Protection Act Legislation.

6.1.4 Effective Services Team

The Effective ServicesTeam will ensure compliance with the SOP for all applicable research or development applications.

6.1.5 Information Governance/

Information Governance Team will provide guidance to support compliance with the National Data Opt-Out Standard Operating Procedure.

6.1.6 Information Team

The Information Team will comply with the the National Data Opt-Out Standard Operating Procedure specifically submitting data sets via the MESH and obtaining a cleansed data set to enable services to comply with the national data opt-out.

6.1.7 Employee's Responsibilities

Employees should take all reasonable measures to comply with the National Data Opt-Out Standard Operating Procedure

7. Monitoring

For this procedure:

- The Information Governance & Data Protection Sub-Committee will monitor compliance with this SOP by way of report of numbers of applicable research of development applications.