Document filename:	**National Data Opt-out Programme - Data Protection Impact Assessment**		
Directorate / Programme	**National Data Opt-out Programme**	Project	**Policy Implementation Workstream**
Status	**Published**	Version	**2.1**
		Version issue date	**24/10/2019**

National Data Opt-out - Data Protection Impact Assessment

Document management

Revision History

Version	Date	Summary of Changes
1.0	14 Sept 2018	Published
2.0	12 Jul 2019	Updated following process updates
2.1	24 Oct 2019	Minor changes following review

Approved by

This document must be approved by the following individuals:

Name	Title	Date	Version
IAO	National data opt-out IAO	21 Aug 2018	0.5
		08 Feb 2019	2.0
		04 Sep 2019	2.1
DPO	NHS Digital DPO	13 Aug 2018	0.4
		12 Jul 2019	2.0
		02 Oct 2019	2.1

Document Control:

The controlled copy of this document is maintained on the NHS Digital 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 5

Introduction 7

1. Consultation with Stakeholders 8

1.1. Types of testing and consultation 8

2. Data Flow Diagram 10

2.1. Setting an opt-out 10
2.2. NHS Digital and DSCROs applying national data opt-outs 11
2.3. Type 2 migration 12
2.4. Reporting and analysis 13
2.5. External upholding 14

3. Purpose of the processing 15

3.1. Overview of the national data opt-out processing 15
3.2. Scope of the data protection impact assessment 16

4. Description of the processing 17

4.1. Policy 17
4.2. Setting and storing national data opt-outs 18
4.3. Applying national data opt-outs by NHS Digital and DSCROs 21
4.4. Transitioning existing opt-outs in line with national policy 22
4.5. Reporting and analysis 22
4.6. Applying national data opt-outs by external organisations 23
4.7. Details of the data stored 24
4.8. Data controllers and processors 25
4.9. Type of data that is processed 25

5. Describe the legal basis for the processing (collection, analysis or disclosure) of data? 25

6. Demonstrate the fairness of the processing 26

7. What steps have you taken to ensure that individuals are informed about the ways in which their personal data is being used? 27

8. Is it necessary to collect and process all data items? 27

9. Describe if personal datasets are to be matched, combined or linked with other datasets (internally or for external customers)? 28

10. Describe if the personal data is to be shared with other organisations and the arrangements you have in place 28

11. How long will the personal data be retained? 29

12. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and, if necessary, kept up to date? 29

13. How are individuals made aware of their rights and what processes do you have in place to manage such requests? 30

14. What technical and organisational controls for "information security" have been put in place? 30

15. In which country/territory will personal data be stored or processed? 31

16. Does the National Data Opt-out apply to the processing 31

17. Identify and assess risks 31

18. Further Actions 40

19. Signatories 40

20. Summary of high residual risks 41

Executive Summary

The national data opt-out service is primarily provided as a mechanism to improve data protection and privacy by offering additional choice to the public about how their confidential patient information is used. The national data opt-out service has undertaken this Data Protection Impact Assessment (DPIA) as good practice. The service is not considered to present a high risk to the rights and freedoms of data subjects that cannot be mitigated and therefore consultation with the ICO is not required.

The national data opt-out was launched in a public beta[1] phase on 25 May 2018 and patients can set a national data opt-out via website, via phone and online (the assisted online service) or by post. NHS Digital has been applying national data opt-outs since 25 May 2018 and work is ongoing with other organisations within health and care to enable them to apply national data opt-outs by March 2020. During the public beta phase, the patient-facing services have been improved and enhanced based on user feedback. The service completed its public beta phase in March 2019 and is now a 'live' service.

The national data opt-out is a policy offer and is in addition to the legal rights afforded by data protection legislation. There are a number of key privacy benefits to the public. It provides a mechanism to opt-out when there may not be any legal right to object. Data subjects only have to express their preference once and by 2020 this will have effect across the health and care system. They do not have to provide any reasons or justification for opting out. These benefits need to be offset against any privacy risks of providing the service itself.

The service has been designed to minimise privacy risks – most notably it uses a single identifier (NHS number) for recording and applying the national data opt-out. The national data opt-out system must strike a balance between appropriate security and verification and ensuring that setting an opt-out is accessible and easy.

In terms of security of the online (and assisted online) system and data repository there is good evidence to support the robustness of arrangements here – although the risk of cyber-attacks remains in the current climate, but no more so than any other online system. There also remains a small risk that someone will maliciously set, or reverse, an opt-out for somebody else without their knowledge. The impact of this is seen to be mitigated by the fact that the essential flows e.g. those which are legally mandated (including safeguarding) are protected. Also, to set an opt-out the user must have a mobile number or an email registered to the Personal Demographics Service (PDS) database. These contact details are used to confirm the opt-out with the individual.

Type 2 opt-outs allowed a patient to object to their confidential patient information being disclosed by NHS Digital for purposes beyond their individual care. All type 2 opt-outs recorded on or before 11 October 2018 were transitioned to national data

[1] A public beta software release is designed to allow a wide group of users to provide feedback on the released software which results in user-driven enhancements to the software during this phase

opt-outs[2]. The transition arrangements carried some limited data protection and privacy risks especially for those who were contacted about their type 2 opt-out.

The main outstanding risk is that the wider public may be unaware of their opportunity to register a national data opt-out. This is being mitigated by the communications plans put in place including posters and handouts which have been widely distributed across health and care settings, and an extensive public information campaign through national newspapers and commercial radio. The wider conversation with the public about the benefits of data and their choices will continue ensuring that there is a consistent narrative as new developments progress – for example the NHS App and Local Health and Care Records. Overall, there is a positive impact on data protection and privacy from the provision of the service. The DPIA will continue to be updated during the life of the programme and when any significant changes occur.

[2] https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/how-we-look-after-your-health-and-care-information/your-information-choices/how-opt-outs-work

Introduction

The Data Protection Impact Assessment (DPIA) has been undertaken during the development of the national data opt-out service to enable NHS Digital to systematically identify and minimise the privacy and data protection risks of the introduction of this new service. The national data opt-out was launched in a public beta form on 25 May 2018. During this public beta period, the service continued to be monitored and improved based on user feedback. The service completed its public beta phase in March 2020 and is now a 'live' service. The DPIA has been updated to cover the additional service that allows organisations to check for national data opt-outs to enable the national data opt-out to be applied by organisations across health and care. This DPIA has been undertaken as good practice for the introduction of a new service which is collecting and processing personal data. The processing required for the national data opt-out service is not considered likely to result in a high risk to the rights and freedoms of data subjects that cannot be mitigated and therefore consultation with the ICO is not required.

The national data opt-out gives people a clear choice about how their confidential patient information is used for purposes beyond their individual care. Individuals can make their choice through a range of channels including online, over the phone and non-digitally. People will be able to express their preference once, and their opt-out will be respected by all health and care organisations by March 2020.

From a privacy perspective, the programme aims to improve individual's privacy by offering a single, simple opt-out that applies across health and care – of particular importance is that it will apply where data can be lawfully processed in circumstances where it may not be practical to seek an individual's consent[3]. It provides a single, central mechanism to opt out of such data uses. The overall model proposed by the National Data Guardian (NDG) is expected to encourage more use of anonymised data which will enhance the privacy of all patients. The national data opt-out is offered in addition to the legal rights afforded by data protection legislation. All data controllers still have to ensure compliance with these requirements, the implementation of the national data opt-out does not change this.

[3] Under the common law duty of confidentiality, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without patient consent. Sec 251 of the NHS Act 2006 recognised that there were essential activities of the NHS, and important medical research, that required the use of identifiable patient information but that it is not always practical to obtain consent - https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/why-confidential-patient-information-used/

1. Consultation with Stakeholders

This impact assessment has been developed in consultation with the following stakeholders:

- National Data Opt-out Programme Team (including security, legal and information governance subject matter experts) drawn from across NHS Digital, NHS England and the Department of Health and Social Care (DHSC)
- National Data Opt-out Programme Board
- Information Commissioners Office (ICO)

See section 4.1 for a more complete list of external stakeholders who have been consulted on the development of the national data opt-out itself.

1.1. Types of testing and consultation

User Testing

The programme has undertaken extensive user and comprehension testing with members of the public, particularly around the most appropriate question for the national data opt-out and testing patients' understanding of what the opt-out is and is not. The outputs of this work have been used to support the DHSC in making key decisions such as the adoption of one question only, the wording of the question itself as well as selecting the terminology that the public best understand.

Private Beta Testing

As part of the private beta testing a number of patients were invited to use the online system. There were approximately 2000 different sessions initiated with just over 500 patients choosing to complete the end to end process and approximately 300 people completing the online survey. User testing has continued during the public beta phase of the programme.

External stakeholders

During the course of the Programme a large number of external stakeholders have been consulted, both in designing the model to be adopted and on specific issues. Most of this consultation was through the Programme Advisory Group[4] and the minutes of these meeting are published. Other stakeholders with specific interests or expertise were consulted on specific issues.

Equality Impact Assessment (EIA)

An equality impact assessment has been conducted which involved extensive consultation with different stakeholder groups, the main aims being to:

- ensure there is equality of opportunity to register a national data opt-out;

[4] https://digital.nhs.uk/about-nhs-digital/our-work/transforming-health-and-care-through-technology/public-trust-and-security-domain-j

- assess any equality risks from differential national data opt-out rates, including whether there might be high rates of national data opt-outs within particular groups and any potential impact this could have;
- ensure that individuals are able to make an informed choice;
- identify any specific policy decisions that may impact upon particular groups with protected characteristics.
- ensure the service is available as widely as possible though providing a number of channels via online, assisted digital and non-digital services.

The EIA is published on the National Data Opt-out Programme webpages[5].

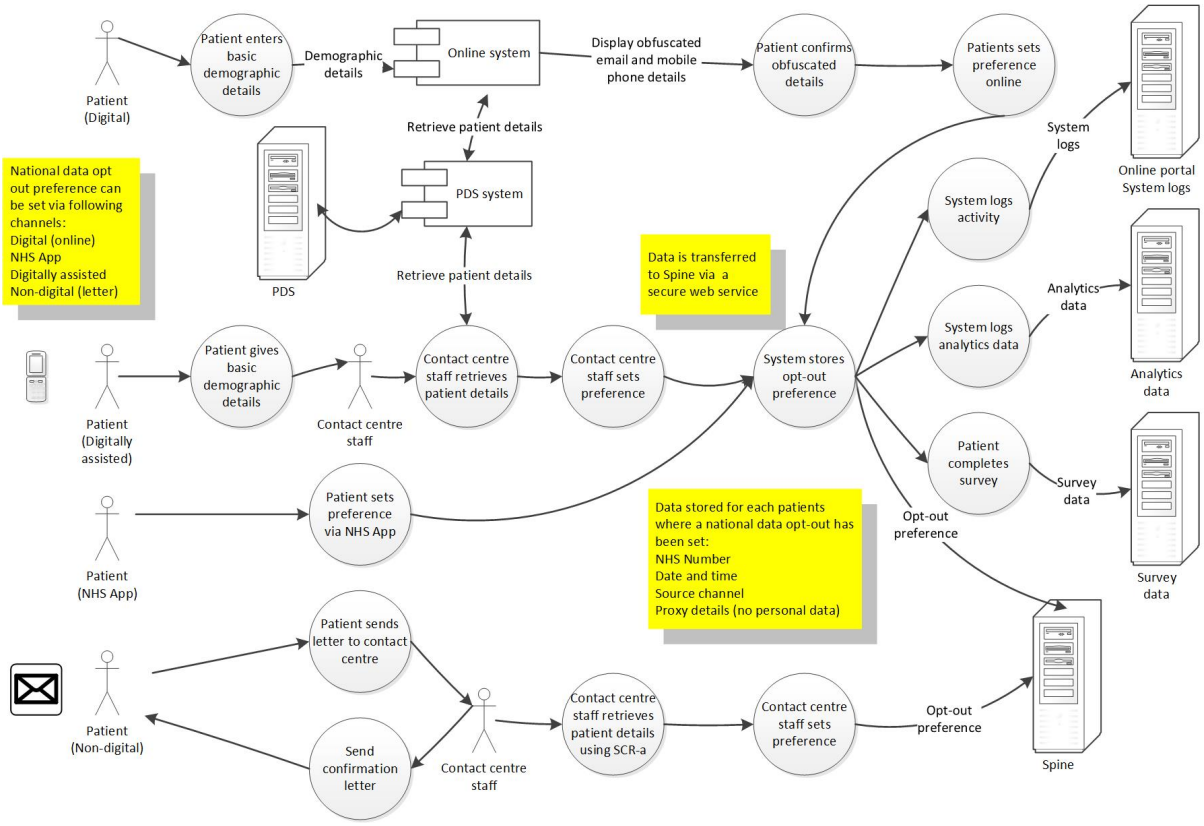
[5] https://digital.nhs.uk/services/national-data-opt-out-programme

2. Data Flow Diagram

The data flows relevant to the national data opt-out processes are presented in the following section.

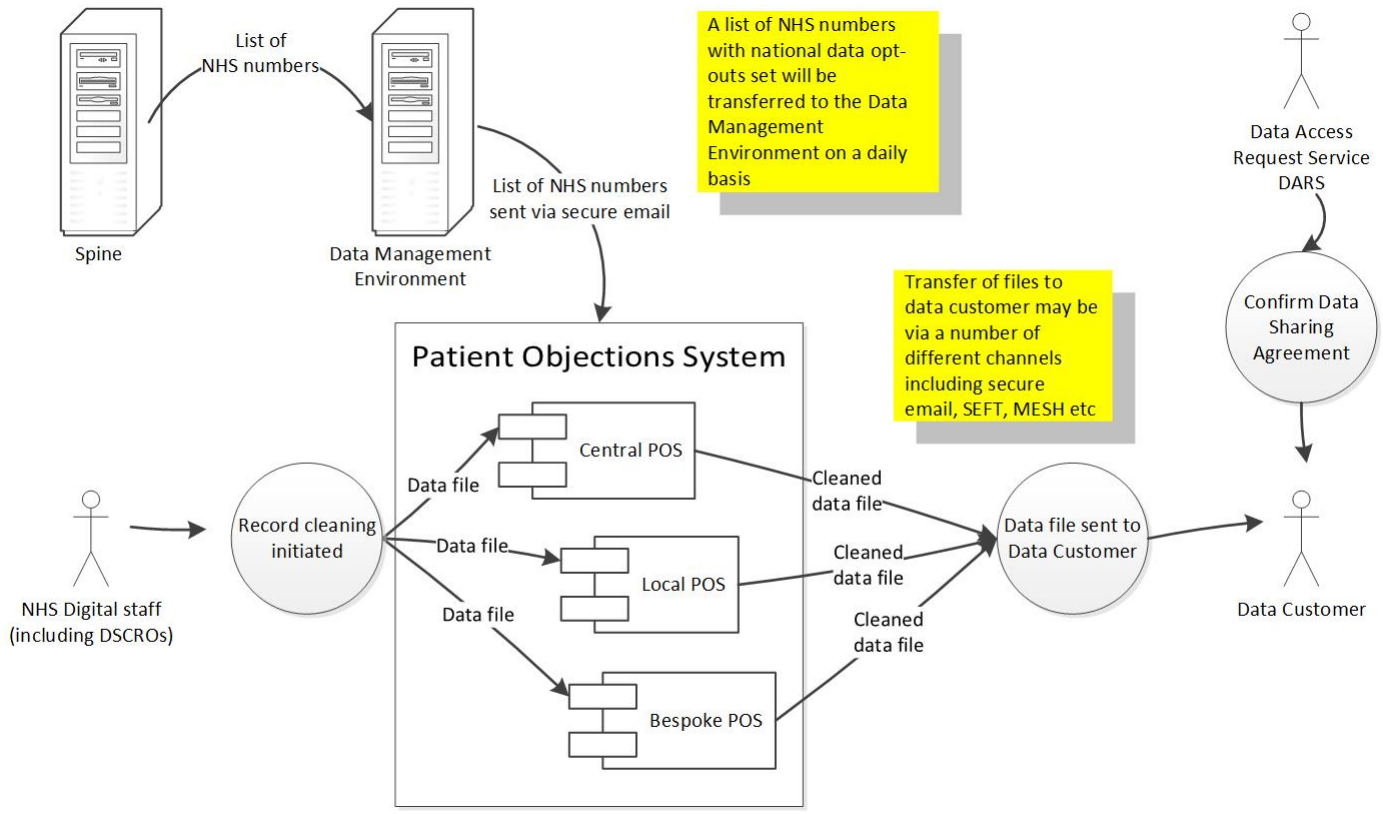
2.1. Setting an opt-out

The data flows required to support a patient setting a national data opt-out:



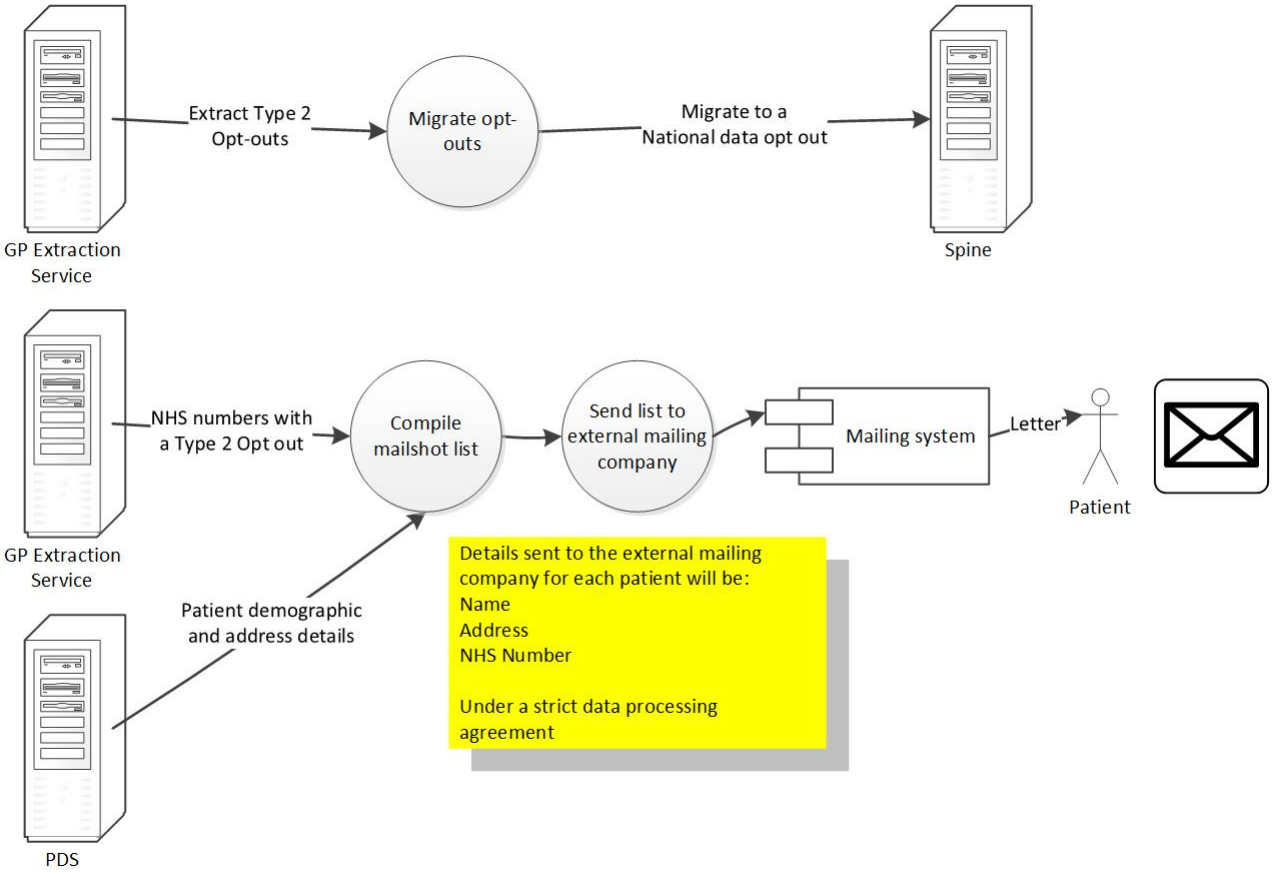
2.2. NHS Digital and DSCROs applying national data opt-outs

The data flows required to support NHS Digital to apply national data opt-outs:



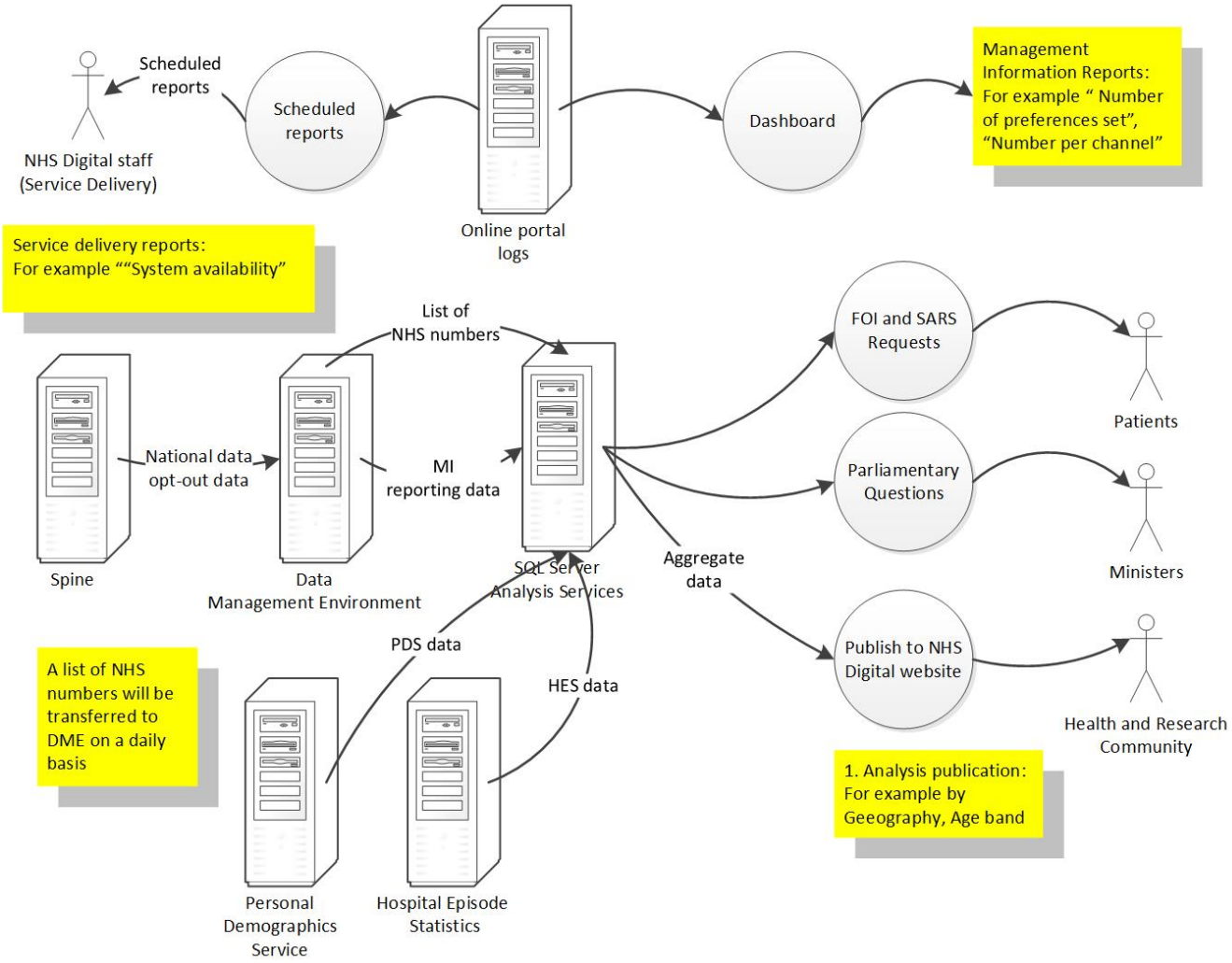
2.3. Type 2 migration

The data flows required to support Type 2 migration:



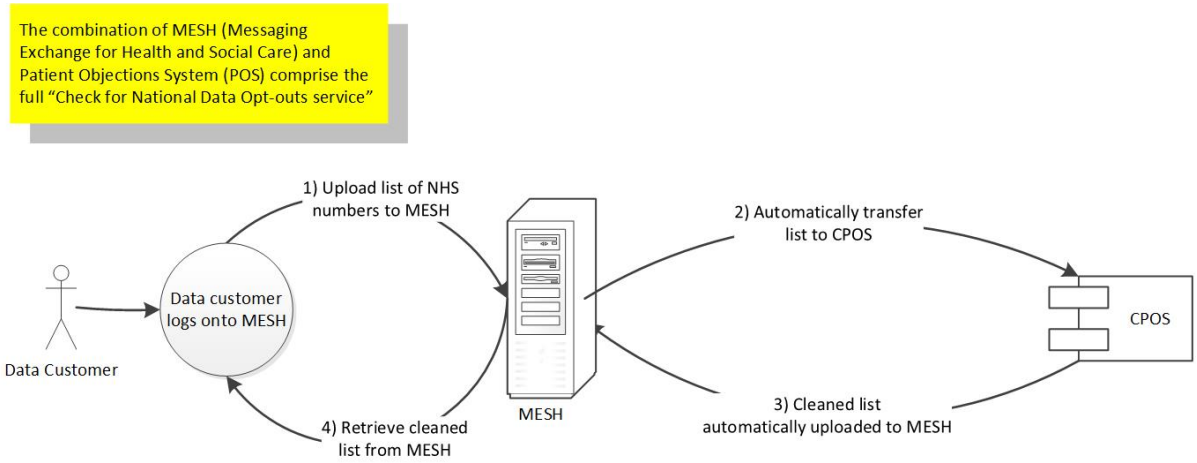
2.4. Reporting and analysis

The data flows required to support reporting and analysis:



2.5. External upholding

The data flows required to support external organisations to apply national data opt-outs:



3. Purpose of the processing

The Government's response to the National Data Guardian (NDG) Review of Data Security, Consent and Opt-outs[6] tasked NHS Digital and partners to implement a national data opt-out to support patient choice about how their data is shared. This comprises:

- Introducing a national data opt-out that the public can set through a range of easily accessible channels;
- Developing and implementing a system to enable all health and adult social care organisations to be compliant with the national data opt-out.

3.1. Overview of the national data opt-out processing

The implementation of the national data opt-out involves the following key elements:

- A system to enable patients to set their national data opt-out both online and by post:
    - An online system implemented by NHS Digital and hosted on the nhs.uk website.
    - The NHS App implemented by NHS Digital.
    - An assisted-online process utilising the online system with phone-based assistance from the contact centre (managed by NHS Digital).
    - An assisted-online process where the individual contacts the contact centre by phone and the contact centre then sets the opt-out on behalf of the individual (managed by NHS Digital).
    - A "by post" (non-digital) contact centre based process (managed by NHS Digital) which provides a non-digital alternative to the channels above to set an opt-out.
- A national repository for storing these national data opt-outs held centrally on the NHS Digital Spine[7]

[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf

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

- Technical solutions enabling national data opt-outs to be applied to national data processing undertaken by NHS Digital[8] both centrally and via the Data Services for Commissioners Regional Offices (DSCROs[9]);
- A technical solution to enable national bodies, local bodies and all health and adult social care providers to apply national data opt-outs to their own data disclosures that are in scope;
- Supporting national bodies, local bodies and health and care providers to declare their compliance with national data opt-out policy.

In addition, existing type 2 opt-outs have been migrated to national data opt-outs. The majority of type 2 opt-outs were migrated in readiness for the launch of the national data opt-out service on 25 May 2018. There was also an agreed transition period up until and including 11 October 2018 where patients could still set a type 2 opt-out via their GP practice. Type 2 opt-outs that were set in this way have also been automatically migrated to national data opt-outs.

In relation to these elements the data protection and privacy impact is considered around five areas.

i) The operational policy guidance that defines the national data opt-out.

ii) Setting and storing national data opt-outs.

iii) Applying national data opt-outs by NHS Digital.

iv) Transitioning existing type 2 opt-outs in line with agreed policy.

v) Applying national data opt-outs by other national bodies, local bodies, and all health and adult social care providers.

3.2. Scope of the data protection impact assessment

The scope of the data protection impact assessment covers all items i) to v) inclusive as described in section 3.1. This impact assessment also covers reporting arrangements including service management, management information and the national data opt-out publications.

Any privacy and data protection risks arising from changes to the underpinning policy will be added on a regular basis in line with the agreed review cycle for the Operational Policy Guidance Document.

A national data opt-out may be set via the NHS App. This data protection impact assessment (DPIA) covers the setting and storing of the national data opt-out via the NHS App but not any other aspects of the NHS App.

[8] This is an uplift to the existing Patient Objection Management System which currently supports the upholding of type 2 opt-outs

[9] The DSCROs are part of NHS Digital, they are not separate organisations. For more information please see https://digital.nhs.uk/services/data-services-for-commissioners-dsfc

The national data opt-out programme assesses the level of risk based on impact and likelihood[10] and by looking at the specific nature of the risk. Where a risk is assessed and considered to present a high risk to the rights and freedoms of data subjects, it is treated as a programme level risk and appropriate mitigating actions are put in place and recorded. The risks identified as part of this impact assessment are documented in more detail in Appendix 1: Risk summary.

The digital channel to set an opt-out is hosted on nhs.uk. The scope of this DPIA covers the national data opt-out and not any of the other services provided on nhs.uk. In addition, although PDS is used as part of the identity verification processes outlined below, no data is updated on PDS as a result of any of the processes described in this DPIA.

4. Description of the processing

The information flows and associated data protection and privacy risks relevant to the national data opt-out policy, setting and storing of national data opt-outs, applying national data opt-outs by NHS Digital, transitioning existing opt-outs in line with national policy and reporting are outlined in the following sections:

4.1. Policy

The national data opt-out policy has been based on:

- the independent and evidence-based review carried out by the National Data Guardian,
- the subsequent public consultation and formal Government response, and
- other specific decisions on scope and exemptions agreed by DHSC

This is a policy offer from the DHSC that provides additional choice for data subjects in addition to the legal rights provided through data protection legislation. The policy has sought to balance the needs of the health and care system and the benefits to individuals and society from sharing health and care data with the provision of increased choice and protection of privacy for individuals. Some aspects may not meet the expectations of every member of society e.g. there are exemptions that will limit the coverage of the national data opt-out. However, these are offset by the provision of clear information to the public when they set their national data opt-out of exactly what the national data opt-out does and does not do. Legal rights remain in place and are unaffected by this policy.

Overall the national data opt-out policy has a positive impact on the privacy and data protection of individuals who interact with the health and care system. Of particular importance is that it will apply where data can be lawfully processed in circumstances where it may not be practical to seek an individual's consent. It provides a single, central mechanism to opt out of such data uses. It is also worth noting that in such cases they may also not have the right to object and as such the

[10] Risk Impact and Likelihood are both assessed on a scale through High, Moderate and Low.

national data opt-out provides an important additional safeguard to the rights and freedoms of data subjects.

4.2. Setting and storing national data opt-outs

The national data opt-out can be set through a number of channels. The processing and relevant data that is utilised by each channel is as follows:

Online Service

The online service requires an individual to verify their identity, set their opt-out and the system then stores this preference centrally. As part of this process, the patient enters the following personal data:

- Name
- Date of birth (DOB)
- NHS number or postcode

User research has indicated that for some patients, a post code may be a more appropriate means to help prove identity than an NHS Number. As a result, from October 2018 a patient has been able to enter a postcode or an NHS number in order to verify their identity.

The system then uses this data (name, date of birth and NHS number or postcode) to uniquely identify the patient on PDS. If an exact match is found, the partial mobile phone number and partial email address details from PDS are presented back to the patient in order to confirm their contact details. These details are currently maintained when a patient has some interaction with the health and care sector with access to PDS, typically in a GP practice.

If the patient accepts the details for one of these contact methods, the system sends a one-time pass-code (OTP) to either the mobile phone or email address. The patient inputs the OTP to access the system and is then able to set (or change) an opt-out. This two-factor authentication ensures the identity of the patient as the mobile phone number or email address must be the one that is registered to them on PDS. None of the data entered by the patient as part of this process is retained.

This two-factor authentication process reduces the risk that another individual can maliciously set or reverse an opt-out for somebody else.

The patient may phone the contact centre who will provide them with verbal assistance as they complete the opt-out process themselves via the online service. The patient enters the required information (as above) but the contact centre is available to respond to any queries or advise on what to do if any problems arise that prevent the patient from completing the process themselves (for example, they do not know their NHS number).

The online service uses cookies to manage each session meaning that some data (including IP Address) is stored in the cookies. This is done to allow NHS Digital to monitor and protect the service from malicious use. The use of cookies is explicitly flagged to a patient at the beginning of the interaction and if the patient does not want to use cookies, they need to use an alternative channel to set a national data opt-out.

NHS App

The NHS App allows a user to view their current national data opt-out setting once they have gained access to the App. The user may elect to change their national data opt-out preference from within the NHS App. The user is not required to enter any additional personal data as part of this process.

Assisted-online (on behalf of) service

The assisted-online “on behalf of” process uses a similar approach and personal data to the online service but the patient first phones the contact centre who enter the personal data on behalf of the patient. The same process is used to send a one-time pass code to the patient in order to validate their identity.

“By post” (non-digital) channel

As part of the by post (non-digital) process to set a national data opt-out, a patient is required to fill in a form and send this to the contact centre via the public postal service. The personal data that the patient is required to submit on the form are:

- NHS number (if known)
- Name
- Address
- Postcode
- Email address (optional)

If the patient is unable to provide an NHS number, they are required to provide copies of two documents to confirm their identity – one for confirmation of name and one for confirmation of address. Valid documents for each purpose are:

- Confirmation of name: full driving licence, passport, birth certificate, marriage certificate
- Confirmation of address: utility bill, bank statement, credit card statement, benefit or pension book

The patient can opt for the contact centre to use their email address to confirm that their opt-out has been successfully updated.

If the opt-out is being set on behalf of somebody else by a proxy (somebody with parental responsibility for a child under the age of 13, a court appointed deputy or somebody with a lasting power of attorney), the proxy is required to submit the NHS number for the patient or (if this is not available) one of the “confirmation of name” documents noted above.

In order to make it easier for those people with parental responsibility to opt-out multiple children, from October 2018, two proxy forms have been made available. One of these is for those with lasting power of attorney or court appointed deputies to submit a proxy opt-out for one patient and another form which allows a proxy with parental responsibility to submit an opt-out for multiple (up to a maximum of 6) children on a single form.

The proxy is also required to provide one each of the “confirmation of name” and “confirmation of address” documents noted above to prove their own identity. Where

the proxy is a lasting power of attorney or a court appointed deputy, they are also required to provide documentation as proof of their authority to act as a proxy. This requires one document from the following list:

- Health and Welfare or Property and Finance Lasting Power of Attorney
- Court of Protection Order (appointing them as a personal deputy)

The parental form has also been updated to include a signed declaration to indicate that the person has parental responsibility rather than having to supply documentation as proof of their authority. This is an approach that has been agreed with the ICO as providing identity to 'prove' parental responsibility (for example a birth certificate) does not guarantee that the person actually has parental responsibility.

The postal process whereby paper forms are sent to NHS Digital was reviewed during the public beta phase and from October 2018 letters are sent to a PO Box where they are delivered directly to the contact centre.

In order to correctly identify the patient on PDS as part of the non-digital process, a member of the contact centre team is able to use the Summary Care Record Application (SCRa) to view the following patient details on PDS. This requires use of a Smart card so that only authorised users have access:

- NHS number
- First name
- Surname
- Date of birth
- Date of death
- Postcode
- Gender
- GP Practice Code

Paper forms received by NHS Digital are scanned and stored electronically for a minimum of three months after they are received. This is considered to be a suitable balance between having sufficient time to allow any follow up queries to the opt-out setting to be addressed but also to not keep personal data for longer than is needed to comply with data protection legislation. The paper forms themselves are destroyed after they have been scanned. Scanned identity documents are also destroyed after they have been used to validate a patient's identity.

There are patient records on PDS where access is restricted in order to safeguard the location and contact details for particular patients. A separate process to set an opt-out has been put in place for those patients via their GP practice and the NHS Digital National Back Office (who are authorised to access such records).

Awareness of the national data opt-out

There is a wider communication risk that patients will not be aware of the availability of a national data opt-out and therefore do not register an opt-out. The communications relevant to the national data opt-out were delivered alongside a wider public communication exercise that emphasised the benefits of data sharing. In addition, the number of patients accessing the different channels to view and set an opt-out is being monitored to ensure the service is available to those who wish to obtain more information or set an opt-out. This is also mitigated by the introduction of

the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018 which requires data controllers to be transparent with data subjects on the data they hold and process.

4.3. Applying national data opt-outs by NHS Digital and DSCROs

Where required, in line with the national data opt-out policy, the systems comprising the Patient Objections Service (POS) are used to remove data from files prior to their disclosure by NHS Digital and Data Services for Commissioners Regional Offices (DSCROs), on the basis of a national opt-out having been set.

The national data opt-out data in the Spine is extracted on a daily basis and transferred to a data warehouse for use by the POS systems. This data is then used as part of the cleaning process to remove any records from files containing confidential patient information where the corresponding patient has a national data opt-out set. This processing is done automatically with no access to view the opt-out data from NHS Digital staff as part of normal operations.

For the systems utilised by the DSCROs, an encrypted list of opt-out settings is sent via secure email to the DSCROs. This encrypted list is then decrypted by the relevant systems for use in the record cleaning process. Again, this is done automatically with no access to view the opt-out data from NHS Digital staff as part of normal operation.

As part of this process, the whole record is removed (not just identifiers) to avoid any risk of re-identification at a later date.

A restricted number of NHS Digital staff have access to the Spine repository or the data warehouse that holds the daily POS extract. This access (which is audited) is only used in exceptional circumstances and must be agreed by the Information Asset Owner.

Any data sent out to data customers is subject to a rigorous governance process managed by the NHS Digital Data Access Request Service (DARS) team. This includes independent scrutiny through the Independent Group Advising on the Release of Data (IGARD) and the creation of a data sharing contract and data sharing agreement (DSA). Please note that national data opt-outs may not be upheld for all data disclosures such as where the data flow is required by law (for example based on CQC statutory powers) or in exceptional circumstances (for example a communicable disease outbreak). These are set out in the National Data Opt-out Operational Policy Guidance Document[11]. NHS Digital publishes a data release register which sets out all data which has been shared, the purpose for which the data was shared and whether the national data opt-out has been applied to a particular release or not.

[11] https://digital.nhs.uk/binaries/content/assets/website-assets/services/national-data-opt-out-programme/guidance-for-health-and-care-staff/ndopnationaldataoptoutpolicy_v2.0.pdf

4.4. Transitioning existing opt-outs in line with national policy

DHSC set out a clear policy to NHS Digital, specifying that existing type 2 opt-outs were to be migrated to a national data opt-out over the public beta period. Patients with an existing type 2 opt-out were informed by letter of the migration and given information about the national data opt-out, including a copy of the patient handout for the national data opt-out. The letters were sent by a third-party mailing company acting under contract as a data processor for NHS Digital. The initial migration took place in time for the launch of the service and the associated communication to patients was done after the national data opt-out public beta launch. Patients could continue to set a type 2 opt-out via their GP practice until and including 11 October 2018 and during this time on a monthly basis NHS Digital carried out additional migration and associated communication to individual patients.

There were some minor privacy risks associated with this process. However, the risk of the patient objecting to this processing was considered preferable to the migration happening without their knowledge or for no migration to take place. Legal cover is provided in the Direction to NHS Digital.

4.5. Reporting and analysis

NHS Digital collects and retains some management information about the performance of the service itself such as time taken for each transaction or system availability. This information does not include any confidential patient information and is used to monitor and improve the service provided.

As part of continuous improvement of the service NHS Digital are using an analytics tool to monitor user activity on the website in order to enable better understanding of user needs and to optimize the service and experience for patients. The analytics tool uses cookies and other technologies to collect data on user behaviour and their devices. The details of these cookies are made clear to the user when they interact with the service. A survey tool is also being used to capture user feedback on the website. A user can enter their name and email address if they consent to be contacted for further feedback about their experience of the site in order to continually improve the user experience. These details will only ever be used for this purpose.

A publication of national data opt-outs is available to the research community and other interested stakeholders and is published on the NHS Digital website. The published analysis is aggregate data only and will never contain any confidential patient information. Further analysis will be added to the publication over time but this will always be done in line with NHS Digital's publication policy[12] and must not contain information liable to identify any one individual.

[12] https://digital.nhs.uk/services/supporting-open-data-and-transparency

Ad-hoc reporting to satisfy freedom of information (FOI)[13] and subject access requests (SARS)[14] and in answer to parliamentary questions will be provided as necessary. However personal data will not be released as part of a freedom of information request where it would contravene data protection principles and stringent identity checks are required before any personal data is released as part of a subject access request.

4.6. Applying national data opt-outs by external organisations

The technical solution to apply opt-outs requires the external organisation to submit a data file containing a list of NHS numbers to the NHS Digital check for national data opt-outs service. This is then 'cleaned' (i.e. national data opt-outs are applied to remove any NHS numbers that are linked with an opt-out) by NHS Digital before it is returned to the external organisation. A more detailed breakdown of the process is as follows:

The data customer from the external organisation logs onto the Message Exchange for Social Care and Health (MESH) and uploads a data file to be cleaned.

The file is automatically retrieved by the check for national data opt-outs service and the file is 'cleaned' to remove any NHS numbers that are linked to a national data opt-out.

The check for national data opt-outs service then returns the 'cleaned' data file to the data customer via MESH.

The data customer from the external organisation then downloads the cleaned file from MESH and can apply the 'cleaned' list to their data disclosure.

The national data opt-out policy allows organisations to submit the list of NHS numbers for their entire cohorts of patients to the "check for national data opt-outs" service and then cache the resulting 'cleaned' list for a limited time period. This is so that this cached list can then be applied to data disclosures for this limited time period. For example, an organisation may choose to submit the list of NHS numbers for their entire cohort of patients to the check for national data opt-outs service each Sunday evening in order to minimise the impact on their technical infrastructure. Where organisations cache data in this way, they are considered to be the data controller for this policy. There are clear policy guidelines on the restrictions that apply to this data including access to the data and the purposes it can be used for and these restrictions are clearly outlined in the licence for the technical solution.

Other solutions were considered, including one whereby external organisations would send a full datafile of patient information to NHS Digital. NHS Digital could then return a 'cleaned' file to the external organisation. However, this presents additional data protection and privacy risks in that this would require disclosure of confidential patient information to NHS Digital. The technical solution chosen is felt to

[13] https://digital.nhs.uk/about-nhs-digital/contact-us/freedom-of-information

[14] https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/publication-scheme/how-to-make-a-subject-access-request

be the best balance between reducing data protection and privacy risks but also minimising burden on external organisations.

Further guidance for organisations who need to be compliant with the national data opt-out, including details of the technical solution are available on the NHS Digital website[15].

There is also a risk that external organisations are not aware of the need to apply national data opt-outs to specific data disclosures. This is being mitigated by an extensive communication and engagement exercise with relevant organisations and their support networks that is raising awareness of the need to be compliant with the national data opt. A comprehensive set of guidance material is available and an Information standard is in place that sets out the requirements that such organisations are required to meet in order to be compliant.

4.7. Details of the data stored

When a patient sets their national data opt-out preference by any of the channels, the choice is stored against their NHS number in the Spine. Different options have been reviewed and the use of NHS number as the primary identifier for an opt-out choice was agreed by the National Data Opt-out Programme Board in order to minimise the privacy risks. In particular to minimise the personal data that is shared with wider health and care system in order to uphold the patient's wishes - but still enable an effective service to be delivered.

The principles of data minimisation are applied to the data that is stored which comprises:

- Setting for the patient's national data opt-out preference
- NHS number
- Channel (via which the opt-out was set)
- Proxy (the type of proxy who set the opt-out but no identifying data for the proxy themselves)
- Date and time the opt-out preference was set.

The preference settings are retained while the national data opt-out remains in place as DHSC policy. Where an individual has never set an opt-out there is no processing of personal data.

A 'history table' is also held which is an audit log of all preference states ever recorded for an individual including the channel, proxy and date and time the opt-out was set. The agreed retention period for the history table is a maximum of eight years from the creation of the audit record (in line with NHS Digital Record Management Policy). At this point this will be reviewed and if necessary a further retention period agreed. The only identifiable data maintained in the history table is the NHS number. The agreed retention period ensures future patient queries can be addressed as completely as possible. Maintenance of the opt-out preferences database history table is undertaken by the NHS Digital Spine team.

[15] https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out

4.8. Data controllers and processors

Tranche 1 of the programme covers the setting and storing of national data opt-outs, applying national data opt-outs by NHS Digital, transitioning type 2 opt-outs in line with national policy and reporting. Tranche 2 of the programme covers the applying of national data opt-outs by external organisations. NHS Digital is a joint data controller (with DHSC) for the national data opt-out service. As such, NHS Digital is required to comply with data protection legislation that defines the responsibilities of a data controller.

A third-party mailing company was engaged to send out the type 2 transition letters and acted as a data processor under contract to NHS Digital.

The analytics tool company are acting as a data processor on behalf of NHS Digital and there is a data processing agreement in place. The survey tool company are acting as a data processor on behalf of NHS Digital. The contract in place with the survey tool company includes a comprehensive data processing agreement that places strict constraints on access to and use of the data that is collected.

Where external organisations are caching lists of NHS numbers to apply to their data disclosures for a limited time period, the external organisation are the data controller for this data and as such are required to comply with data protection legislation that defines the responsibilities of a data controller.

4.9. Type of data that is processed

For the purposes of setting a national data opt-out, a patient is required to submit a number of items of personal data (name, date of birth, address, post-code and NHS number). However, it does not include any data that would be considered “special category data” under the GDPR.

5. Describe the legal basis for the processing (collection, analysis or disclosure) of data?

A Direction to NHS Digital from DHSC (dated 12th September 2017) provides the legal basis for the collection, analysis and disclosure of national data opt-out data. The direction provides legal instruction covering the following activities:

- Collect the patient national data opt-out data
- Establish a national repository for central storage of the patient national data opt-out data
- Establish a system to enable health and care organisations to access the national data opt-out data
- Write to patients with a type 2 opt-out to inform them of the transition to the national data opt-out
- Undertake analysis of the patient national data opt-out data (this may include linking the patient opt-out data to other patient data held by NHS Digital)
- Contact patients with an opt-out if there are significant changes to the national data opt-out policy

A second direction dated 21 May 2018 provides the start date for the service and sets out the transition arrangements for type 2 opt-outs. The direction provides legal instruction covering the following activities:

- NHS Digital to start to operate the system to uphold national data opt-outs
- NHS Digital to publish and maintain policy guidance
- Organisations providing health services or adult social care will be responsible for applying the national data opt-out in line with the published policy and timetable set by DHSC
- Type 2 objections to be converted to national data opt-outs

For more information please see the NHS Digital Directions[16] webpage.

The technical system to enable health and care organisations to apply the national data opt-out will require organisations to send lists of NHS numbers to NHS Digital who will then remove any NHS numbers associated with a national data opt-out before returning the 'cleaned' list to the organisation.

The full legal basis for the collection, analysis and disclosure of personal data (for the activities defined above) under GDPR is as follows (please note that this is different for the return of the 'cleaned' list to the organisation):

Article 6(1)(c): processing is necessary for compliance with a legal obligation to which the controller is subject;

OR (for the return of the 'cleaned' list to the organisation:

Article 6(1)(e): processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Article 9(2)(h): management of health and social care

6. Demonstrate the fairness of the processing

In order that there is no breach of confidence, at the point of setting a national data opt-out the patient has been informed and had their expectations clearly set as to how their Confidential Patient Information will be used.

[16] https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions

7. What steps have you taken to ensure that individuals are informed about the ways in which their personal data is being used?

A link to the privacy notice[17], nhs.uk website terms and conditions and nhs.uk cookie information are provided when setting via the online and through the assisted-online services. These make it clear what personal data is collected, how it is processed and what is retained – this includes setting out how opt-out and associated audit data may be used for analytical purposes and to allow organisations to apply national data opt-outs. Based on testing with members of the public and service user experience surveys, the comprehension levels for the service are good.

A copy of the privacy notice is provided to those using the by post (non-digital) service.

8. Is it necessary to collect and process all data items?

Data Items	Justification
Name	The patient's name that is entered as part of the identity verification process for the digital, digitally-assisted and non-digital channels is not stored after the process has been completed. The name of any proxy is also not stored after the process has been completed.
Address	The patient's address is captured on the non-digital form and is used in contacting patients and other correspondence from the contact centre. The address of any proxy is not stored after the process has been completed.
Postcode	The patient's postcode may be used as part of the identity verification process for the non-digital channel and is not stored after the process has been completed.
Date of birth	The patient's date of birth is used as part of the identity verification process for the digital, digitally-assisted and non-digital channels and is not stored after the process has been completed.
Date of death	Date of death is not collected as part of the identity verification process but may be viewed by the contact centre team in order to ensure that the opt-out is not being set for a patient who is deceased in line with the policy.
Proxy confirmation	Any copies of documents used to prove a proxy relationship will not be stored after the process has been completed.
Email Address	The patient's email address may be used to contact the patient as part of the digital channel opt-out setting process.
General Identifier e.g.	The patient's NHS number is used as part of the identity verification process for

[17] https://your-data-matters.service.nhs.uk/privacynotice

Data Items	Justification
NHS No	the digital, digitally assisted and non-digital channels. The value entered by the patient is not stored at this point, but if the patient elects to set an opt-out, this will be stored against the NHS number once the process is complete.
Home Phone Number	In certain circumstances the NHS Digital contact centre may be required to take a contact telephone number for a patient in order to get back in touch with them with further information. This process is covered by rigorous process controls
Online Identifier e.g. IP Address / Event Logs	IP addresses will be stored in system logs to monitor for suspicious activity and potential malicious opt-out
Website Cookies	Website cookies are used to temporarily store a session identifier, but the cookies are deleted either on termination of the session or after 1 month or 365 days, depending on the cookie. The cookies are used to store device details relevant to the session. Users are made aware of the use of cookies when they visit the website.
Mobile Phone / Device Number	The patient's mobile phone number may be used as part of the identity verification process for the online channel and is not stored after the process has been completed.

9. Describe if personal datasets are to be matched, combined or linked with other datasets (internally or for external customers)?

NHS number is the only identifier used for the purposes of applying the national data opt-out. No linkage to other data sets is required for NHS Digital to apply the opt-out although PDS is used as part of the identity verification process.

Analysis of the potential impact of opt-outs for data disclosures will be published to support data recipients. This will be done by linking with PDS and Hospital Episode Statistics (HES) data but no identifiable information from PDS or HES will be used. This and any other analysis will be undertaken in a way that prevents the identification of an individual with a national data opt-out.

10. Describe if the personal data is to be shared with other organisations and the arrangements you have in place

In order for external organisations to be able to apply national data opt-outs to relevant data disclosures, the "Check for National Data Opt-outs service" is provided to enable organisations in health and adult social care to comply with the national data opt-out policy. The service takes an input list of NHS numbers and returns a 'cleaned' list of NHS numbers where any NHS numbers in the input list with a

national data opt-out are removed from the 'cleaned' list. It is acknowledged that the service could be used to try and identify the national data opt-out preference for a patient. The "Check for National Data Opt-outs service" licence puts a number of restrictions on the use of the service in order to minimise the risk of national data opt-out preferences for patients being revealed. Please see the Check for national data opt-outs service licence[18] for further details.

11. How long will the personal data be retained?

The national data opt-out preference for a person will be held until they change their mind and update their choice on the system or until DHSC instructs NHS Digital to no longer run this service. If DHSC policy changes such that the national data opt-out is no longer required, the opt-out preferences will be anonymised or deleted when they are no longer needed in line with NHS Digital's records management policy. The audit history of a patients opt-out setting will be retained for a maximum of eight years from the point at which the setting was changed in line with NHS Digitals' record management policy.

General cookie data is deleted after the session ends or after 15 minutes if the sessions ends unexpectedly. The cookie that is used to determine whether to display the cookie warning message (that alerts users to the cookie policy) is stored for 1 month. The cookies used by the analytics tool (that prevent polls and feedback forms being presented back to users who have already seen them) are stored for 365 days. The survey data collected from the survey tool is stored for a maximum of 3 years.

Once copies of identity documents have been used to prove the identity of a person, the documents are securely destroyed. No electronic copies of the identity documents are maintained. Any original identity documents sent in error to the contact centre are returned to the sender via recorded delivery post. The paper forms used to set an opt-out are stored for a minimum of 3 months after the opt-out has been set.

12. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and, if necessary, kept up to date?

The national data opt-out choice setting is held on Spine to indicate if a patient has set an opt-out choice. Individuals will receive a confirmation text/email or letter when their transaction is completed that confirms their opt-out status. The patient will be able to view their setting at any time and will be able to change their opt-out preference if they believe it to be incorrect via any of the channels.

For the purposes of NHS Digital applying the opt-out, the list of national data opt-outs is updated in the internal POS systems that apply the opt-out on a daily basis.

[18] https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out/check-for-national-data-opt-outs-service/licence

The list of national data opt-outs is sent to the relevant systems used by the DSCROs in applying the opt-out on a weekly basis.

Where the contact details (email address or mobile phone number) that are stored on PDS for a patient are either incorrect or not present, the patient may have these details updated by a healthcare professional where their internal systems can synchronise with PDS. This would typically be done by the patient contacting their GP practice.

13. How are individuals made aware of their rights and what processes do you have in place to manage such requests?

This data is collected and processed under Directions using the processing condition that “processing is necessary for compliance with a legal obligation to which the controller is subject.” The rights data subjects can exercise are:

- Right to be informed – this is met through the information provided at the time of registering an opt-out and through the privacy notice sent to them or published on NHS Digital’s website. The landing pages for the service have a direct link to the privacy notice.
- Right of access – the opt-out can be set and viewed directly by the public via the online system or through the telephone helpline. On completion of each transaction the user gets a confirmation (SMS, email or letter) which confirms their national data opt-out status.
- Right to rectification – the opt-out can be reviewed and directly amended by the data subject via the online system or through the telephone helpline. On completion of each transaction the user gets a confirmation (SMS, email or letter) which confirms their national data opt-out status.
- Right to restrict processing (where an individual contests the accuracy of the personal data) - the opt-out can be set and viewed directly by the data subject via the online system or through the telephone helpline.

This is a policy offer which is accessed and controlled directly by the data subject in setting, viewing and amending their own opt-out status. Individuals can change their mind at any time and remove their national data opt-out. These rights and how to access them are set out in the privacy notice and on the NHS Digital website.

14. What technical and organisational controls for “information security” have been put in place?

The Spine has a comprehensive service management and information security plan defined and is securely protected by firewalls and other security mechanisms hence the risk of losses due to cyber-attacks are considered to be low. For further details please see Appendix 1: Risk summary.

15. In which country/territory will personal data be stored or processed?

The national data opt-out preference for a patient is held on the Spine. This is maintained on servers that are hosted within the EEA.

16. Does the National Data Opt-out apply to the processing

The purpose of the programme of work is to enable national data opt-out preferences to be set by patients and these opt-out preferences to be applied where required by organisations within health and adult social care.

17. Identify and assess risks

The following section sets out the detailed risk assessment for different aspects of the national data opt. The pre and post mitigation risk ratings are included. For some risks, existing mitigation measures (for example relating to Spine security) were already in place prior to the start of the programme of work:

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Date security and integrity				
Data could be subject to cyber-attack	High Moderate	Tolerate	• Spine service management and information security plan. • Annual penetration tests run by the Spine service teams. • Access and controls applied as if this was clinical data.	High Low

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Unauthorised access or loss	Moderate Low	Tolerate	• Existing Spine access controls. • NHS Digital policies and procedures on access to data. • NHS number data is extracted and applied automatically with no human intervention. • NHS Digital terms and conditions for staff. • Potential “value” of opt-out data is considered low. • Also see specific risk “External organisations can determine who has an opt-out”.	Moderate Low
Information asset unavailable	Moderate Low	Tolerate	• Spine target of 99.9% availability. • Spine service management and information security plan.	Moderate Low
Cloud hosted solution (data loss and cyber attack)	High Low	Tolerate	• Only transient data stored on the cloud. • Represents a “Class 1” risk (the lowest level). • Cloud servers are hosted in the European Economic Area (EEA).	High Low
Data stored by analytics and survey tools	Moderate Low	Treat	• Used to help monitor and improve the service. • Data only stored in anonymised form. • Data is stored in the EEA. • Data processing agreement in place that limits use of the analytics and survey data.	Low Low
Legal basis				

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Legal basis for processing	Moderate Low	Tolerate	• Directions from DHSC provide the legal basis for processing. • Minimum audit data required for processing is stored. • Clear privacy information ensures 'no surprises'.	Moderate Low
Type 2 migration				
Contacting patients by letter may be seen by some as an invasion of privacy	Moderate Moderate	Treat	• A transparent and open approach is preferable to the migration happening without patients' knowledge. • Patients' feedback during DHSC consultation that they would expect their type 2 opt-out to be migrated. • Legal cover provided in the Direction to NHS Digital. • Approach discussed and agreed with a range of stakeholders including the ICO.	Moderate Low
PDS address information may be incorrect or patient may have died	High Low	Treat	• Data extracted from PDS at as late a date as is practically possible. • Lists match to date of deaths data. • Process allows a forwarding address to be returned.	Moderate Low
Patient does not know they have a type 2 opt-out	High Low	Treat	• GP Practices were contacted in advance.	Moderate Low

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Address information sent to the mailing company may be lost or stolen	High Low	Tolerate	• Transfer of patient data via a secure and encrypted channel. • Strict contractual agreements prohibiting any other use of the data.	High Low
Type 2 opt-outs set after national data opt-out launch	Moderate Low	Tolerate	• Communications to GPs. • Ongoing migration to national data opt-outs for Type 2 opt-outs set up to and including 11 October 2018.	Moderate Low
Malicious Opt-out				
An opt-out may be set or reversed maliciously	Moderate Moderate	Treat	• Identity checking required to set an opt-out including two-factor authentication requiring a single exact match on PDS based on entered details (name, date of birth and NHS number or postcode) • Benefits from doing so are low. • Essential flows including communicable diseases and safeguarding are protected. • Formal risk assessment undertaken and kept under review.	Moderate Low
Communications				

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Patients not aware of the opt-out	High Low	Treat	• Extensive public communications plan at launch involving national newspapers, commercial radio adverts and targeted black and minority ethnic channels. • Sustainable communication plan to be developed over time using the learning from the launch and public beta. • GDPR strengthened transparency requirements. • Numbers of patients accessing the opt-out service is under continual review to ensure there are no barriers to setting an opt-out.	Moderate Low

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Certain groups not able to set a national data opt-out	Moderate Moderate	Treat	• Extensive public engagement undertaken with groups representing range of accessibility needs. • Equality Impact Assessment (EIA) conducted. • Work with the voluntary sector resulting in tailored resources (including easy read, large print, audio, Braille and British Sign Language and other languages resources). • Tailored resources for specific audiences including Black and Minority Ethic (BME) patients, carers and young people. • Translation of materials. • Extensive accessibility testing via the Digital Accessibility Centre (DAC)	Moderate Low
Setting an opt-out				
Making demographic data available for identity verification	Low Low	Tolerate	• Feedback provided during user testing did not identify an issue. • Many individuals felt it was important to provide enough information so that the opt-out was correctly allocated to them.	Low Low
Communication details for patients being revealed	Low Low	Tolerate	• Minimal (obfuscated) email and mobile phone details are presented back to the patient. • Reasonable balance of risk vs benefit opinion tested in public beta.	Low Low

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Contact centre staff may enter personal details incorrectly	Low Low	Tolerate	• One-time pass code returned to patient minimises risk of error.	Low Low
Patient data may be lost or stolen in transit	Low Low	Tolerate	• The mail is sent to a PO box and then directly accessed by contact centre staff. • This is not seen as a high risk for theft in transit e.g. there is no money or other valuables accompanying the paperwork.	Low Low
Location details may be disclosed for PDS records where access is restricted	High Medium	Treat	• A separate process for sensitive records has been put into place for such patients.	Medium Low
Copies of identity documents may be accessed by unauthorised personnel	Moderate Low	Tolerate	• Document copies are stored securely. • Document copies destroyed after use. • Original documents returned to sender via recorded delivery.	Moderate Low
NHS Digital applying opt-outs				
The opt-out may not be applied when required by the policy	Low Low	Tolerate	• Replaces similar process to apply type 2 opt-outs within NHS Digital. • User interface design, user documentation and staff training delivered.	Low Low
Policy				

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Definitions and exemptions limit coverage	High High	Treat	• Scope of the model and a number of broad exemptions were proposed by NDG based on an independent and evidence-based review. • Other specific decisions on scope and exemptions agreed by DHSC to balance ensuring health and care system can continue to have information it needs to run effectively and efficiently and providing choice about how data is used. • Clear information is provided on the landing pages including details of the specific exemptions and that the opt-out applies to England only.	High Low
Opportunities or privacy benefits				
Significant positive impact on privacy	N/A	Tolerate	• Additional choice to the public about how their confidential patient information is used in addition to legal rights. • Data subjects express their preference once and do not have to approach many different data controllers separately. • No justification is needed. • Applies when legal rights may not.	N/A

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
More complete and accurate patient contact details on PDS through patients requesting updates to their records	N/A	Tolerate	• Facilitates future communications to patients. • Enhances the security of any access to their data. • Compliance with the fourth data protection principle that personal data shall be accurate and, where necessary, kept up to date.	N/A
External upholding solution				
External organisations can determine who has an opt-out	Low Medium	Treat	• Service licence restricts what organisations can use the opt-out data for.	Low Low
External organisations may not respect fair processing times	N/A	Transfer	• Communications materials available clearly detail the fair processing timeframe.	N/A
Data may be lost or hacked in transit	Medium Medium	Treat	• NHS numbers alone are not considered to be very 'valuable' to hackers. • Data transfer is via MESH which is a secure encrypted transfer channel.	Medium Low
Minimise data transfer as part of the solution	N/A	N/A	• Alternative technical solutions considered including one where entire file of patient data sent to NHS Digital for 'cleaning' • Chosen solution felt to give the best balance between minimising data protection and privacy risks and minimising burden	N/A

Risk (grouped by category)	Pre Impact / Likelihood	Risk Decision	Risk Notes, Mitigation and Treatment	Post Impact / Likelihood
Remove entire record from dataset	N/A	N/A	• Whole record to be removed from dataset when applying the national data opt-out to minimise the risk of re-identification • Other options considered included only removing identity fields	N/A
Organisation awareness of the need to be compliant with the national data opt-out	High Medium	Treat	• Extensive communication and engagement exercise to raise awareness of the need to be compliant • Information standard that defines the requirements • Extensive range of guidance material available	High Low

18. Further Actions

This DPIA will be revisited during the lifecycle of the project / programme to ensure:

- Outcomes and measures identified are still relevant
- Action treatments recommended to mitigate risks are implemented
- Mitigating actions are successful

The DPIA will be revisited at regular intervals during the on-going live period.

19. Signatories

The IAO should sign and date here to confirm that the DPIA accurately reflects the processing and they are happy to accept the residual risks of the processing

Name, job title and signatory	Date
Tim Magor, Digital Delivery Director	29/07/2019

20. Summary of high residual risks

No residual high risks remain.

All DPIAs which indicate a high risk(s) shall be reviewed by the Office of the SIRO and further advice will be sought from the Office of the Data Protection Officer (DPO). Approval for the processing must be sought from the SIRO and DPO and their opinion documented.

The GDPR requires that where a DPIA indicates that processing operations involve a high risk which cannot be mitigated by appropriate measures in terms of available technology and costs of implementation, a consultation with the Information Commissioners Office (ICO) should take place prior to the processing. The DPO will conduct this consultation. **This is required prior to the implementation of any high-risk processing activities**

Upon consultation the ICO, as supervisory authority under the GDPR, is able to exercise its powers under the GDPR and may investigate, enforce correction, sanction or authorise such processing operations. Such powers also include the power to impose a temporary or definitive limitation or ban on processing.