Data Protection Impact Assessment (DPIA)

A DPIA is a legal requirement and should be completed when sharing personal information, for example when commissioning a new service, working on a specific project/process/scheme or implementing a new system; **or** when making changes to any existing service/project/process/scheme. The DPIA must be completed at the start of the project to provide the Trust with the key assurances on data protection requirements and enable the Trust to evidence accountability in all activities.

Project name:

Implementation of the National Data Opt-Out by Moorcroft Medical Centre

Name of Project Lead and Job Title

Donna Talbot, Informatics Manager, Moorcroft Medical Centre

Date of Completion of DPIA

18/02/2022	

Section 1 – Initiation Phase

1.1 Project outline – what and why

Note: Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The service to apply national data opt-outs to data disclosures requires additional processing of confidential patient information. As this is classed as "special category data" as defined under the Data Protection Act 2018/UK GDPR and can involve processing data on a large scale as well as matching to the national opt-out data which comes from a different source, it is considered relevant, in line with the guidance on when to complete a DPIA, to undertake a DPIA to understand and mitigate the additional data protection risks this might. Compliance with the National Data Opt-Out is required by all health and social care organisations by March 31st 2022, which includes all GP Practices. If the national data opt-out is not correctly applied the Information Commissioner's Office have stated this could be treated as a breach of the Data Protection Act 2018 (DPA18) requirements for processing to be fair and transparent. If the processing results in unauthorised access to patient data this could be treated as a breach of the DPA18 requirements that cover unauthorised or unlawful processing of sensitive personal data.

National data opt-outs apply to purposes beyond individual care. For common law purposes, the sharing of information for direct or individual care purposes is on the basis of implied consent, which falls outside of the scope for national data opt-out. In the case of explicit consent, where an individual has explicitly consented to the use of their personal information, for example, consenting to be part of a research study, this would fall within the general exemption for national data opt-out and this rule applies even if the consent was given before the individual had set a national data opt-out. If there is a mandatory legal requirement to share patient information, then the national data opt-out will not apply.

Information disclosure that has Section 251 support obtained under Regulation 2 (diagnosis and treatment of cancer) or 5 (medical purposes set out on the schedule for the regulations) of the Control of Patient Information Regulations will ensure the national data opt-out applies unless the Confidentiality Advisory Group (CAG) have advised:

- That the national data opt-out is overridden in the public interest (in exceptional circumstances only)
- 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, the National Cancer Register or the National Congenital Anomaly and Rare Diseases Register.
- Data disclosed under Regulation 3 (communicable diseases and other risks to public health) is exempt from the national data-opt out.

It is essential when determining whether the national data opt-out applies to determine the purpose, which must be beyond individual care, as well as the basis for disclosure in common law.

1.2 Use of personal data

The national data opt-out applies where section 251 support, which enables the use of confidential patient information (CPI) without consent, is relied upon and guidance is provided. CPI is defined in sections 251 (10) and (11) of the National Health Service Act 2006. Broadly it is information that meets all of the following 3 requirements:

- identifiable or likely identifiable (for example from other data likely to be in the possession of the data recipient)
- given in circumstances where the individual is owed an obligation of confidence
- conveys some information about the physical or mental health or condition of an individual, a diagnosis of their condition; and/or their care or treatment.

It should be noted that Section 251 (also known as S.251) has been updated to ensure that the definitions used expressly include local authority social care (i.e. care provided for, or arranged by, a local authority). The term confidential patient information (CPI) also covers data which falls within the "special categories of personal data" under article 9 UK GDPR and indeed goes beyond this as it also covers information about the deceased whereas the UK GDPR only applies to living individuals.

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

The national data opt-out **does not apply** to **workforce or staff data**. NB: Staff data may be removed as a result of the opt-out being applied but only where it is relevant to a patient's care (for example, a consultant's name may be linked to an episode of care).

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

1.3 Describe the nature of the processing

Note: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The national data opt-out was introduced to give patients a choice on how their confidential patient information is used for purposes beyond their individual care.

The information that the opt-out applies to is special category data as it includes information about a patient's health care and/or treatment that has been collected as part of the care we provide for the patient.

Patients can set or change their national data opt-out choice using an online or contact centre service. When a patient sets a national data opt-out it is in held in a repository on the NHS Spine against the patient's NHS number.

In accordance with the patient's wishes and national data opt-out policy, as a GP Practice located in England, we are required to apply national data opt-outs when applicable to a use or disclosure of confidential patient information for purposes other than the patient's care or treatment, for example for planning or research purposes.

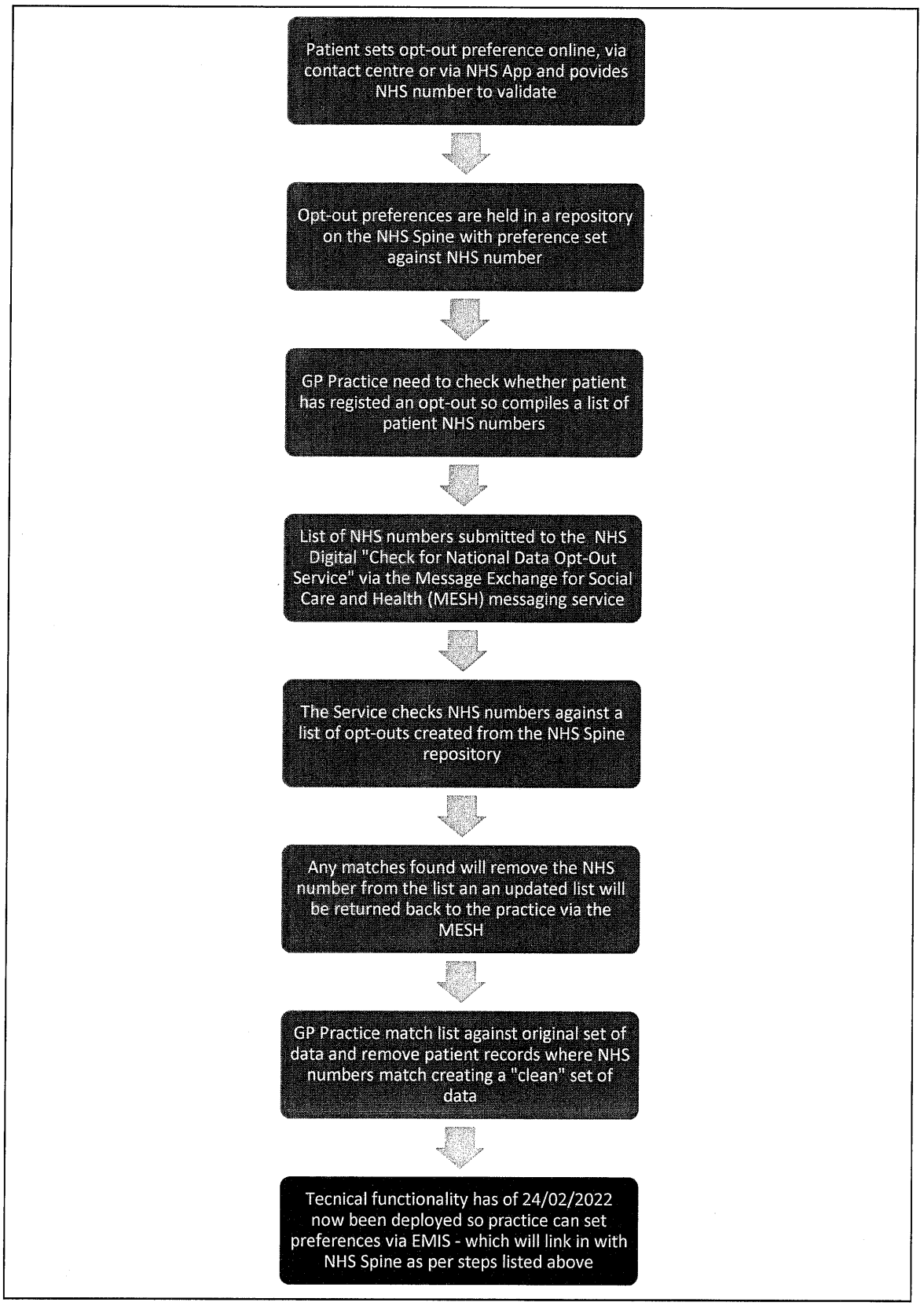
Applying the opt-out to a data use/disclosure requires that we check, by using the NHS numbers of patients, whether a patient has registered an opt-out before the data is used/disclosed.

To do this a separate list of the NHS numbers in the data that is going to be used/disclosed needs to be created. The list of NHS numbers is then submitted to the Check for National Data Opt-outs service via the secure Message Exchange for Social Care and Health (MESH) messaging service. The Check for National Data Opt-outs service is an external service provided by NHS Digital. The service checks the list of NHS Numbers against a list of opt-outs created from the repository on the NHS Spine, where a match is found it removes the NHS number from the list and then returns an updated list of NHS numbers (with opt-outs removed) back to us via MESH.

We then match the updated list of NHS numbers against our original set of data that was going to be used/disclosed and remove the entire record for those patient records where the NHS numbers match. This creates a 'cleaned' set of data with opt-outs applied that we can then use/disclose." As the GP Practice is serviced by the EMIS system the processing described above will be carried out automatically by the system as of 24/02/2022 when the functionality to set opt-outs is deployed in the system.

The National Data Opt-Out may take up to 21 days from a preference being registered with NHS Digital to being fully applied to all disclosures of data and the service to check for opt-outs is updated every 24 hours.

1.3.1 Data Flow Diagram



1.4 Data Controller/Processor Responsibilities

Note: What are the responsibilities linked to the processing? Who is the Data Controller, are there any Data Processors, Sub-Processors or any Joint Data Controllers?

The GP Practice is a data controller, and have responsibilities for ensuring that patient information is handled, processed and shared in the most appropriate way. The practice adheres to all data controller responsibilities and has taken all appropriate steps to demonstrate compliance with National Data Opt-Out. NHS Digital via facilitation of the MESH service and NHS Spine will be processing data on behalf of the practice under strict requirements in their role as data controller, but retain their own data controller status.

Section 2 - Compliance with privacy laws

Note: Data Protection legislation is relevant to any DPIA, and a DP compliance check should always be carried out. The Data Protection Officer will be able to advise you on the relevance of other privacy laws.

2.1 UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA)

Note: The template you have to fill in for the data protection compliance check can be found in Appendix A of this document. The Trust Information Governance Team will be able to assist with the completion, prior to approval granted by the Trust Data Protection Officer, SIRO and Caldicott Guardian.

A Data Protection compliance check has been carried out as part of this DPIA, the details of which are in appendix A. From this we have concluded: Risks have been mitigates as per the risk matrix and this DPIA helps to demonstrate compliance with NDO.

2.2 Human Rights Act (HRA) (Article 8)

Note: In most cases HRA considerations will be covered by the other work on this DPIA, including the Data Protection compliance check. If that is the case, you can simply record here that there are no special considerations that are not covered by other aspects of the DPIA. If there are any outstanding issues, describe them here.

As individuals have a choice on whether to share their data for planning and research purposes, their human rights have not been infringed and individuals are encouraged and empowered to make their own decisions on how their information is used, so would not constitute a breach of human rights. However when implementing any process that involves personal information the Human Rights Act is reviewed in tandem with data protection legislation, all relevant codes of practice and the 8 Caldicott Principles.

2.3 Privacy and Electronic Communications Regulations 2003 (amended 2011) (PECRs)

Note: If the project involves electronic marketing messages (by phone, email or text), cookies, or providing electronic communication services to the public, you also need to make sure you comply with the PECRs.

The following guidance will help: Information Commissioner's Office PECR guidance.

Describe any issues here, or confirm if not applicable.

The purpose for processing information in relation to the National Data Opt-Out does not constitute direct marketing and as such there are no PECR considerations with this DPIA.

2.4 Common Law Duty of Confidentiality

All staff employed by the GP Practice, as well as those employed by the NHS regardless of the organisation, are compelled to adhere to the common law duty of confidentiality at all times and ensure staff are understanding that whenever they hands, process and share personal information, they do so with strict codes of confidentiality integral to their day-to-day activities and must not disclose any information without the correct legal basis applied.

2.5 Other legislative requirements

DCB3058 Information Standard published under Section 250 of the Health and Social Care Act 2012

Section 3 – Technological requirements

3.1 Technology

3.1.1 What systems/assets will be used to support the project?

Note: Please list all software, hardware and information assets associated with this project

Software Assets GP System – EMIS MESH (if required as a back up to EMIS enabled functionality to set opt-out preferences) NHS Spine **Hardware Assets** Practice desktop PCs/laptops/any device with capability to connect to the internet **Information Assets** DPIA National Data Opt-Out Policy Privacy notices – compliance statement within the privacy notice. Opt-Out Resources produced by NHS Digital

3.2 Data collection

3.2.1 Will the project involve the collection of new information about individuals?

Yes: ☐

No: ☒

3.2.2 Will the project compel individuals to provide information about themselves during the course of the project?

Yes: ☐

No: ☒

3.3 Identification methods

3.3.1 Will there be new or different identity authentication requirements?

Yes: ☒

No: ☐

3.4 Involvement of external organisations

3.4.1 Will the initiative involve external organisations that will have access to the personal data?

Yes: ☒

No: ☐

3.5 Changes to the way data is handled – considering the actual processing

3.5.1 Will there be new or significant changes to the handling of special categories of personal data or data that would be considered sensitive by the data subjects? *(For example, data about racial/ethnic origin, political opinions, health information, sexuality, offences and court proceedings, finances etc.)*

Yes: ☒

No: ☐

3.5.2 Will the personal details about each individual in an existing database be processed in a new or different way?

Yes: ☒

No: ☐

3.5.3 If yes to the above, will this involve a large number of individuals?

Yes: ☒

No: ☐

3.5.4 Will the project use an automated-decision-making tool? *(Note automated-decision making is a computer generated decision making tool based on algorithms that make decisions without a human being)*

Yes: ☒

No: ☐

Section 4 – Pre-implementation

Note: Explain below what checks will be carried out before the service/project/scheme/system is implemented to ensure that the privacy solutions approved as part of this DPIA have been applied, and that the system or process is still legally compliant. Also include whether data subjects have been appropriately informed.

National Data Opt-Out Compliance deadline is March 31st 2022, so prior to this deadline the practice will ensure all procedures are in place against the operational policy guidance as detailed in the following link: https://digital.nhs.uk/services/national-data-opt-out/compliance-with-the-national-data-opt-out

Section 5 – Review

Note: Indicate below how and when the post-implementation review will be carried out:

Prior to implementation and following compliance deadline

To be undertaken by:

The Practice

Date review required:

Prior to 31/03/2022

4.1 Formal Approvals

Note: All DPIAs must go through rigorous checks before receiving formal approval. Approval is received from the Trusts Data Protection Officer, Senior Information Risk Owner and Caldicott Guardian (where applicable).

Data Protection Officer Approval:

LIZ GRIFFITHS
Print Name

18/02/2022
Date of Approval

Senior Information Risk Owner Approval:

CHRIS BIRD
Print Name

24.02.22
Date of Approval

Caldicott Guardian Approval:

Print Name

STEPHEN PARNELL

Date of Approval

Appendix A

Data Protection Compliance Schedule

Completion of this schedule requires knowledge of Data Protection Legislation, including adherence to the Data Protection Act 2018/ UKGDPR. Assistance can be obtained from the Trust's Information Governance Team NSCHT.informationgovernance@combined.nhs.uk

	Question	Answer
1.	What type of personal data will be processed? (Please list every data requirement)	NHS Number
2.	What is the legal basis for processing the personal information for the given purpose? (Please provide the relevant legal basis from Article 6 of the UK GDPR as shown via the link – https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/#what)	The legal basis under UK GDPR and the DPA18 for us to send and receive NHS numbers (considered personal data but not special category data) to and from the Check for National Data Opt-outs service provided by NHS Digital is based on the following: **Article 6(1)(c): processing is necessary for compliance with a legal obligation to which the controller is subject** as detailed in **Sections 254(1), (6), 274 (2) of the Health and Social Care Act 2012.**
3.	When processing special category data (i.e. health, sexuality, biometric data, religion etc.) enhanced privacy measures are applied, as the processing of such data is prohibited in principle. To enable this data to be shared, Article 9 of the UK GDPR lists lawful grounds for processing this type of data. Which article 9 exemption applies to this scheme/project/process/system?	Article 9(2)(h) of UK GDPR allows for processing for **"management of health and social care based on member state law"**: which is provided for in the **DPA18** Schedule 1 Paragraph 2 (2) (f): "**The processing is necessary for the management of health care systems or service or social care systems or services and is processed by or under the responsibility of a health professional or a social work professional, or by another person who owes a duty of confidentiality under an enactment or rule of law."**
4.	Are there any special considerations relating to Article 8 of the Human Rights Act that will not be covered by the DPIA?	As individuals have a choice on whether to share their data for planning and research purposes, their human rights have not been infringed and individuals are encouraged and

	Note – This Article provides that everyone has the right to respect their private and family life, their home and correspondence. It is subject to qualifications relating to national security, crime etc.	empowered to make their own decisions on how their information is used, so would not constitute a breach of human rights. However when implementing any process that involves personal information the Human Rights Act is reviewed in tandem with data protection legislation, all relevant codes of practice and the 8 Caldicott Principles.
5.	If consent is the lawful basis for processing the data, how will consent be obtained and how will you ensure it meets the definition of consent as detailed in the DPA18? (*Note: consent must be specific, explicit, an unambiguous indication of the data subjects wishes, validated by clear affirmative action or written statement*)	The opt-out does not apply when the individual has consented to the sharing of their data or where the data is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice on Anonymisation. Consent is not the lawful basis.
6.	Will any of the personal data be processed under Common Law Duty of Confidentiality? If yes, how is that confidentiality being maintained?	All staff employed by the GP Practice, as well as those employed by the NHS regardless of the organisation, are compelled to adhere to the common law duty of confidentiality at all times and ensure staff are understanding that whenever they hands, process and share personal information, they do so with strict codes of confidentiality integral to their day-to-day activities and must not disclose any information without the correct legal basis applied.
7.	How are individuals informed of how their personal data will be used?	The practice advertises National Data Opt-out including the signposting to the online service, contact centre and NHS App for setting opt-out preferences both online and in practice via the use of NHS Digital resources provided to raise awareness for all patients. A section of the practice privacy notice is dedicated to the National Data Opt-Out to ensure patients are appropriately informed
8.	Does the project involve the use of personal data for purposes other than those listed in this DPIA?	This DPIA is purely for the National Data Opt-Out and for the process detailed in this DPIA only NHS number will be used and only for purposes that

		meet the criteria for national data opt-outs to be applied.
9.	How can data subjects exercise rights in relation to access to their own records?	National Data Opt Outs are applied to a patient record via the NHS number so if a patient wishes to access their own personal information via a Subject Access Request the record will detail that the national data opt out applies – all requests will be facilitated via the GP Practice who have a robust Subject Access Request Policy and accompanying procedures in place to ensure all requests are handled in line with data protection legislation.
10.	How can the rights of data portability be met safely and effectively?	The right to data portability only applies when the lawful basis for processing patient information is consent **or** for the performance of a contract, and as these are not the lawful bases relied on for the purposes of the National Data Opt-Out this right will not apply.
11.	How can data subjects exercise their rights to rectification and/or erasure?	Given the national data opt out is based on the individuals preferences, unless the national data opt-out has been applied to the incorrect NHS number which would require immediate rectification by the practice this would not be routinely applied.
12.	How can data subjects exercise their right to restrict data flows or object to the processing of their data?	If a patient at any pint changes their mind on their National Data Opt Our preferences they can amend their preferences online, via the contact centre or via the NHS App, or inform the GP Practice of this. This will ensure the process as detailed within this DPIA will be followed.
13.	What procedures will be in place to ensure that the data requirements are adequate, relevant and limited to what is necessary in relation to the purpose for which the data will be processed? (data minimisation)	In order to respect and apply national data opt-outs in accordance with patient wishes it is necessary to check patient NHS numbers using the Check for National Data Opt-outs service and to process confidential patient information further in order to be able to apply national data opt-outs as described earlier. Only the minimum amount of data required i.e. the NHS

		number is used to check if a national data opt-out is held.
14.	How will the data be kept accurate and up-to-date at all times?	It is the responsibility of all individuals to ensure they inform the GP Practice of any changes to their personal details to ensure information is held accurately and up-to-date. The Practice will then ensure they adhere to their robust policies on data quality to ensure information is maintained at all times.
15.	Is there concern that sharing the personal data to inform this project/process/scheme/system could cause upset/distress to the data subjects? If so please add how this will be addressed.	The National Data Opt-Out is aimed at empowering individuals to make choices in relation to their own personal data and be involved in the decision making on how their data is used – as such this should not cause harm, upset or distress but the practice have a responsibility on ensuring as much information as possible is provided to individuals to aid in their decision making.
16.	What is the retention period in relation to the storage of the personal data?	National Data Opt-Out wills be applied to the GP Record and form part of the patient electronic record, which has a retention period of lifetime of the patient and 10 years after death, as stipulated by the NHS Records Management Code of Practice 2021.
17.	What technical and organisational security measures will be in place to prevent any unauthorised or unlawful processing of the personal data?	NSCHT have robust technical measures in place to protect against infiltration, loss, destruction or damage through anti-virus software, two factor authentication methods, rigorous access measure and controls, regular audits of confidentiality as well as evidence and accountability with any suppliers that we use. The GP Practice are required to complete to satisfactory standards, the online self-assessment tool on confidentiality entitled the Data Security and Protection Toolkit, a yearly submission to NHS Digital which demonstrates accountability and compliance in all key governance processes of which integrity and confidentiality of systems is a fundamental requirement. NSCHT

		have recently been awarded DCB1596 accreditation for the way they transfer data via email systems, which have the same technical measures in place as those of an nhs.net email address providing key assurances on the transfer of data. NSCHT is registered with the ICO with renewal of registration due in November 2022. All staff are trained on an annual mandatory basis in Information Governance and every staff member is issued with an IG/Data Protection Handbook and supported by a team of specialist IG staff with a Data Protection Officer in place to oversee compliance. All organisations involved in this process are required to demonstrate that they too have the appropriate technical and organisational measures in place to ensure when transferring data it is safe.
18.	If there is a Data Processor/Sub-Processor involved, are the obligations of the Processor clearly defined in a contract?	A Data Processing Agreement/Contract will not be required for the National Data Opt-Out as agreements are in place with NHS Digital who operate as a national safe haven for patient information with specific powers under the Health and Social Care Act 2012, allowing for the safe transfer of information from the GP Practice to NHS Digital for specified purposes.
19.	Does data get transferred outside of the United Kingdom and if so where? Also what provisions will be in place for data transfers outside of the UK?	No data is held at practice level of via NHS Digital in part of their processing requirements will leave the UK and as such there are currently no additional considerations for transfer of data outside of the UK.

NHS
North Staffordshire
Combined Healthcare
NHS Trust

Appendix B - Data Protection Impact Assessment Risks

Risk description	Inherent Privacy Risk			*Options for avoiding or mitigating this risk	Risk Owner	Residual Privacy Risk		
	Impact	Likelihood	Exposure			Impact	Likelihood	Exposure
Lack of knowledge or understanding about national data opt-out policy results in national data opt-outs not being applied or being applied incorrectly to a data disclosure.	Low	Low	Low	The GP Practice will ensure that relevant staff are aware of and trained in the requirements of the national data opt-out policy. Practice procedures and policies for existing and new data disclosures and staff training will be updated in order to take account of the national data opt-out. For further help and guidance please see the National data opt-out: compliance implementation guide.	GP Practice	Low	Low	Low
A 'data processing person', who is not authorised is able to access confidential patient information when	Low	Low	Low	Wherever possible, the processes to create lists of NHS numbers or applying 'cleaned' lists to disclosures should be	GP Practice	Low	Low	Low

NHS
North Staffordshire
Combined Healthcare
NHS Trust

creating the list of NHS numbers to send to the service and when applying the list of NHS numbers to a data disclosure.				automated so that there is no need for any additional personnel to have direct access to confidential patient information. If these processes cannot be automated ensure there's a procedure in place so only authorised personnel are involved with this processing and that there are defined and documented roles relevant to this processing.				
Technical issues with EMIS functionality	Low	Low	Low	EMIS have now developed the automated process of assigning national data opt-outs at practice level and must ensure staff in practice are appropriately informed and understand how to utilise the system to perform the national data opt-out functionality – any ongoing issues regarding technical	**EMIS/ Practice staff**	Low	Low	Low

NHS
North Staffordshire
Combined Healthcare
NHS Trust

				functionality to be handled by EMIS direct.				
While the Check for National Data Opt-outs service is being used confidential patient information may be accessed by unauthorised personnel, accidently deleted, destroyed or damaged because the prepared data disclosure is not stored securely.	Low	Low	Low	Consider technical security measures (for example, encrypting devices where the data is stored), managing user access rights and ensuring networked areas have the correct view and write permissions.	**GP Practice**	Low	Low	Low
Where multiple data disclosures are being prepared for release over a short period of time an incorrect 'cleaned' list of NHS numbers from the service may be applied to a data disclosure, resulting in national data opt-outs not being applied correctly.	Low	Low	Low	Ensure organisational policies and procedures and staff training are clear and recommend checks are implemented to make sure the correct 'cleaned' lists are applied to the correct data disclosures. Processes should propose the 'Local id' that is used as part of the Check for National Data Opt-outs service is also used as a unique identifier for each data disclosure so that it is	**GP Practice**	Low	Low	Low

NHS
North Staffordshire
Combined Healthcare
NHS Trust

				clear the two files relate to each other. If automated processes are in place to apply opt-outs to data disclosures, make sure the system is tested to cope with more than one data disclosure at a time and consider putting checks in place to ensure that all NHS numbers in the 'cleaned list' are actually present in the data disclosure.				
A data processor acting on behalf of the organisation does not apply national data opt-out policy correctly resulting in national data opt-outs not being applied or being applied incorrectly to a data disclosure.	Low	Low	Low	It is the responsibility of the data controller to ensure that national data opt-outs are applied in line with the policy. A data processing agreement (DPA) must be in place with the data processor that stipulates how decisions are made on applying national data opt-outs and who is responsible for the processing of those opt-outs along with stipulations on controls	**GP Practice/DPO**	Low	Low	Low

NHS
North Staffordshire
Combined Healthcare
NHS Trust

				over who will have access to the data required to undertake the processing to create the data disclosures. Ideally the processing should be automated as much as is practically possible.				