

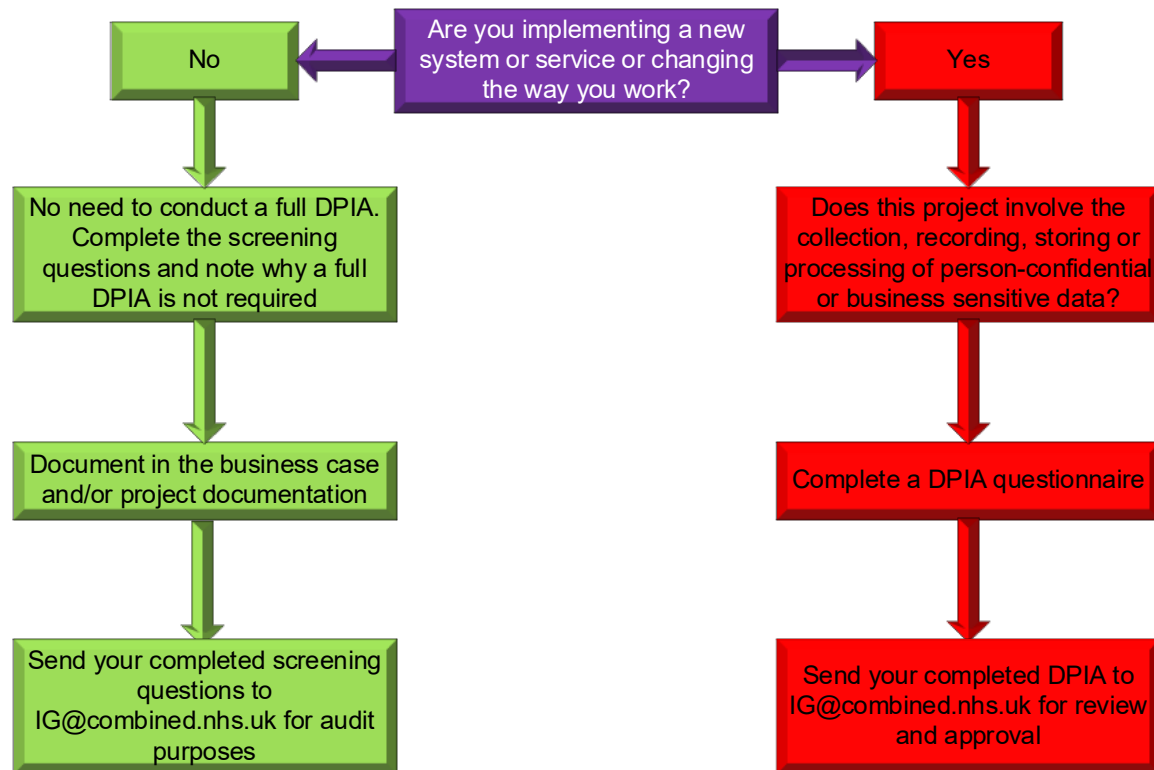
# Data Protection Impact Assessment Questionnaire



# 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.

Use the flowchart below as a guide if you are unsure whether or not to complete this template.



## Section 1: Is a DPIA needed?

Name of Project	National Data Opt-Out for Moorcroft, Holmcroft and Keele GP Practices.
Purpose of the Project/Service <i>Please include benefits and expect outcomes</i>	<p>With effect from 31<sup>st</sup> March 2022, all health and social care organisations, including GP Practices, were required to comply with the National Data Opt-Out which was introduced to give patients a choice on how their confidential patient information is used for purposes beyond direct care.</p> <p>The National Data Opt-Out applies where section 251 support (s.251) 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 which enables the use of confidential patient information (CPI) without consent, is relied upon.</p> <p>This is information that meets the following requirements:</p> <ul style="list-style-type: none"> <li>• Identifiable or likely identifiable (for example from other data likely to be in the possession of the data recipient</li> <li>• Given in circumstances where the individual is owed an obligation of confidence</li> <li>• 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.</li> </ul> <p>The term confidential patient information (CPI) also covers data which falls within the 'special categories of personal data' under article 9 UKGDPR and also covers information about the deceased whereas the UKGDPR only applies to living individuals.</p> <p>For common law purposes, the sharing of information for direct or individual care purposes is on the basis of implied consent, which falls outside the scope for the National Data Opt-Out.</p> <p>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 the 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 does not apply.</p> <p>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:</p>

	<ul style="list-style-type: none"> <li>• That the National Data Opt-Out is overridden in the public interest (in exceptional circumstances only)</li> <li>• 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</li> <li>• Data disclosed under Regulation 3 (communicable diseases and other risks to public health) is exempt from the National Data-Opt-Out</li> </ul> <p>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.</p> <p>The National Data Opt-Out does not apply to information that is anonymised or to workforce or staff data.</p> <p>The National Data Opt-Out relates to information about an individual's health and social care in <b>England only</b>.</p> <p><b>This DPIA is an update of the previous version, which only referenced Moorcroft.</b></p> <p>Holmcroft and Keele GP Practices integrated into NSCHT on 1<sup>st</sup> January 2022 and 1<sup>st</sup> October 2023 respectively.</p>
Name of Project Lead and Job Title	Sahra Smith, Head of Information Governance and Trust Data Protection Officer.
Name and Job Title of the person completing the DPIA	Sahra Smith, Head of Information Governance and Trust Data Protection Officer.
<b>Timescales for the Project/Service</b>	
When is the project/service due to begin? If its time limited, please note the expected end/review date	Already in progress – ongoing.
<b>Key Contacts</b>	
Stakeholders	NSCHT. Moorcroft, Holmcroft and Keele GP Practices. NHS England.
<b>Screening Questions – tick as appropriate</b>	
<b>Information Type</b>	<b>IG Use Only</b>
1. No person identifiable or corporate sensitive information is being used	<input type="checkbox"/>
2. Personal information is being used	<input checked="" type="checkbox"/>
3. Special Category information is being used	<input type="checkbox"/>
4. Criminal Offence information is being used	<input type="checkbox"/>

5. Corporate Sensitive information is being used	<input type="checkbox"/>	
<b>Information Source</b>		<b>IG Use Only</b>
6. Information source - Patient	<input checked="" type="checkbox"/>	
7. Information source - Staff	<input type="checkbox"/>	
8. Information source – Other	<input type="checkbox"/>	
9. The individuals' are children or other vulnerable groups	<input checked="" type="checkbox"/>	
<b>Information Collection &amp; Uses</b>		<b>IG Use Only</b>
10. It is possible to do this work without using personal information	<input type="checkbox"/>	
11. It is possible to use pseudonymised data for some elements of processing – provide details ( <i>which elements, technique to be used and re-identification prevention</i> )	<input type="checkbox"/>	
12. New information about individuals will be collected	<input type="checkbox"/>	
13. Information will be used for a purpose it is not currently used for, or in a way it is not currently used	<input type="checkbox"/>	
14. The information is of a kind particularly likely to raise privacy concerns	<input type="checkbox"/>	
15. New technology will be used that might be perceived as being privacy intrusive	<input type="checkbox"/>	
16. Information will be disclosed to organisations or people that have not previously had routine access to the information	<input checked="" type="checkbox"/>	
17. Direct Marketing will be used	<input type="checkbox"/>	
18. Individuals will be contacted in a way that they may find intrusive	<input type="checkbox"/>	
19. Decisions will be made, or actions taken against individuals in ways that could have a significant impact on them	<input type="checkbox"/>	
20. Indirect access to personal confidential data will be allowed	<input type="checkbox"/>	

## Section 2: Controller/s<sup>1</sup> and Processors<sup>2</sup>

Name of Organisation	Controller or Processor	Completed and compliant with the DSP Toolkit? <sup>3</sup>	IG Use Only
Moorcroft, Holmcroft and Keele GP Practices	Individual Controllers - each GP Practice is a data controller and is responsible for ensuring that patient information is handled, processed and shared in the most appropriate way.	Yes <input checked="" type="checkbox"/> No <input type="checkbox"/>	

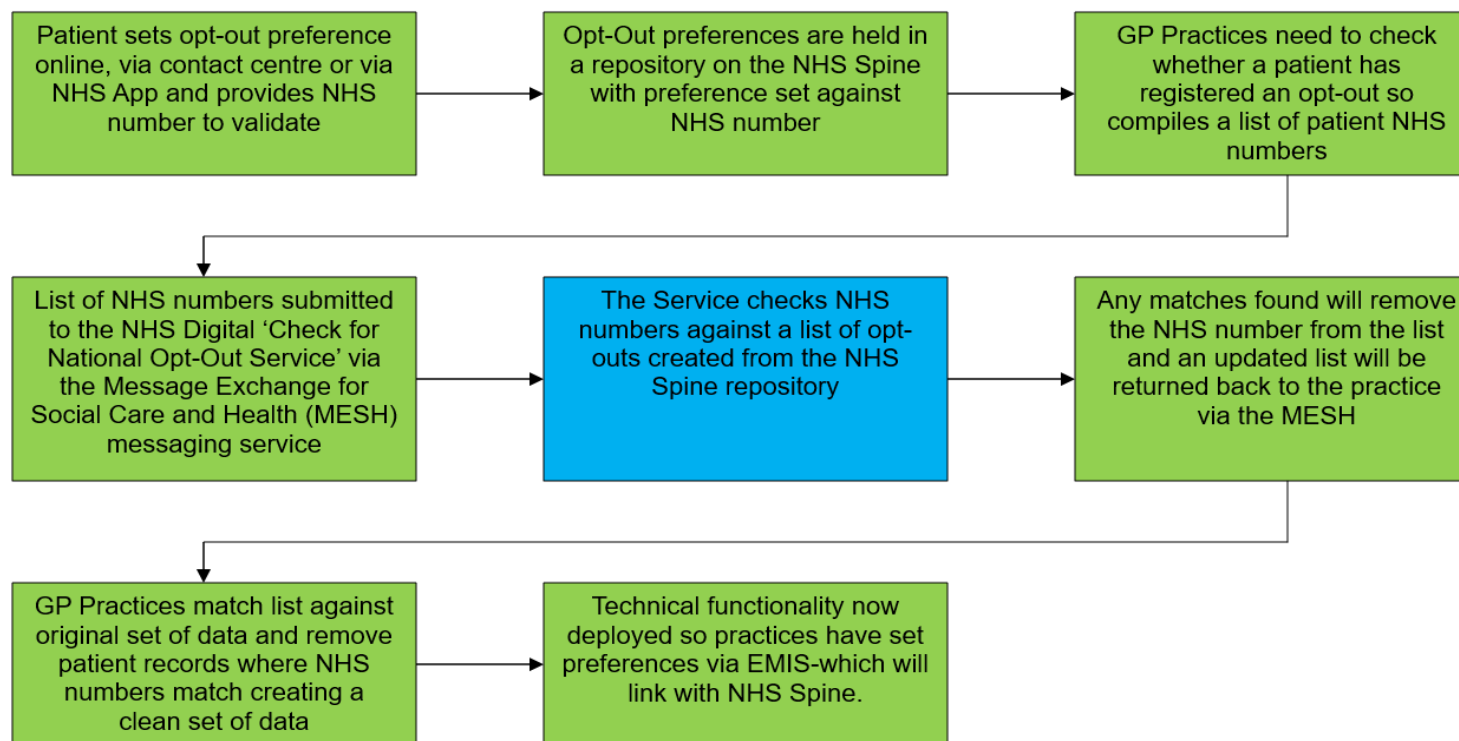
<sup>1</sup> 'Controller' means alone or jointly with others, the organisation that determines the purposes and means of the processing of personal data – for example, this is the case where an organisation is obliged by law to carry out a specific function

<sup>2</sup> 'Processor' means alone or jointly with others; the organisation processing personal data under the instruction of a Controller and does not determine the purposes and means of processing personal data

<sup>3</sup> The Data Security and Protection Toolkit is a self-assessment tool provided by NHS Digital to assess compliance with the 10 National Data Guardian Security Standards

	The Practices adhere to all data controller responsibilities and take all appropriate steps to demonstrate compliance with the National Data Opt-Out.		
NSCHT	Arms length Controller by virtue of Primary Care Integration.	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>
NHS England	Processor - NHSE via facilitation of the MESH Service and NHS Spine process data on behalf of the GP Practices under strict requirements in their role as data controllers but retain their own data controller status.	Yes <input checked="" type="checkbox"/>	No <input type="checkbox"/>

Describe the process flow:



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

Regulation and Assurance - tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Organisations are registered with the ICO	<input checked="" type="checkbox"/>		
Organisations are not ISO27001 certified	<input type="checkbox"/>		
DTC has been completed and supplied (embed here)	<input type="checkbox"/>		
Contracts contain necessary IG clauses	<input type="checkbox"/>		
Regular pen testing is required	<input type="checkbox"/>		

### Section 3: Personal Data<sup>4</sup>

Which types of personal data items do you need to use and why? Tick all that apply			IG Use Only
Data Item Types		Why do you need to use them?	
Forename	<input type="checkbox"/>		
Surname	<input type="checkbox"/>		
Address	<input type="checkbox"/>		
Postcode Full	<input type="checkbox"/>		
Postcode Partial	<input type="checkbox"/>		
Date of Birth	<input type="checkbox"/>		
Age	<input type="checkbox"/>		
Gender	<input type="checkbox"/>		
Physical description (i.e., height)	<input type="checkbox"/>		
Phone Number	<input type="checkbox"/>		

<sup>4</sup> 'Personal Data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Email Address	<input type="checkbox"/>		
GP Details	<input type="checkbox"/>		
Legal Representative name	<input type="checkbox"/>		
NHS Number	<input checked="" type="checkbox"/>		
National Insurance Number	<input type="checkbox"/>		
Other numerical identifier	<input type="checkbox"/>		
Photograph/picture of people	<input type="checkbox"/>		
Location Data (i.e., IP address)	<input type="checkbox"/>		
Audio Recordings	<input type="checkbox"/>		
Video Recordings	<input type="checkbox"/>		
None	<input type="checkbox"/>		
<b>Which types of special category data items do you need to use and why? Tick all the apply</b>			<b>IG Use Only</b>
<b>Data Item Types</b>		<b>Why do you need to use them?</b>	
Physical or Mental Health	<input type="checkbox"/>		
Biometric information in order to uniquely identify an individual	<input type="checkbox"/>		
Genetic Data such as a DNA sample	<input type="checkbox"/>		
Sexual Life or orientation	<input type="checkbox"/>		
Racial or ethnic origin	<input type="checkbox"/>		
Political Opinions	<input type="checkbox"/>		
Religious or philosophical beliefs	<input type="checkbox"/>		
Trade Union Membership	<input type="checkbox"/>		
Criminal or suspected criminal offences	<input type="checkbox"/>		
None	<input type="checkbox"/>		
<b>Conditions for processing personal data: to be identified as to whether they apply</b>			<b>IG Use Only</b>
<b>Condition</b>	<b>Tick all that apply</b>		
Explicit consent unless or allowed by another legal route	<b>Explicit consent</b> <input type="checkbox"/>	<b>Another legal route</b> <input checked="" type="checkbox"/>	
We have a contractual obligation		<input type="checkbox"/>	
We have a legal obligation		<input checked="" type="checkbox"/>	
We have an obligation to protect someone's life		<input type="checkbox"/>	

We need it to perform a public task	<input type="checkbox"/>	
We have a legitimate interest	<input type="checkbox"/>	
We need it to comply with our legal obligations for employment	<input type="checkbox"/>	
We need it for legal claims, to seek legal advice or judicial acts	<input type="checkbox"/>	
We need to comply with our legal obligations to provide information where there is a substantial public interest	<input type="checkbox"/>	
We need it to comply with our legal obligations to provide or manage health or social care services	<input checked="" type="checkbox"/>	
We need it to comply with our legal obligations for public health	<input type="checkbox"/>	
We need it for archiving, research and statistics where this is in the public interest	<input type="checkbox"/>	
We have Section 251 support from the Secretary of State for Health and Care or HRA following an application to the Confidentiality Advisory Group (CAG). Please provide CAG reference number:	<input type="checkbox"/>	
<b>Processing of Personal Confidential Data – provide details below</b>		<b>IG Use Only</b>
How much data will you be collecting and using?	NHS number only	
Please confirm that you will be using only the minimum amount of personal data that is necessary	Yes – only the NHS number is used.	
Describe the checks that have been carried out regarding the adequacy, relevance and necessity for the collection of personal & sensitive data	It is the responsibility of all individuals to ensure they inform the GP Practices of any changes to their personal information to ensure that it is up to date and accurate. The Practices ensure that robust processes are in place around data quality.	
How often will you be collecting the data?	As necessary	
Who will be able to access identifiable data?	GP Practice Staff.	
How many individuals are affected?	Undetermined.	
What geographical area does it cover?	North Staffordshire.	
What is the nature of your relationship to the individuals?	Patient/Health Provider.	
How much control do individuals have and would they expect their data to be used in this way?	Complete control – their choice.	
Describe how any issues of public concern should be factored into the use of information for this purpose	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.	

How long are you planning to use the information?	The National Data Opt-Out preference will be used until the individual changes their mind and update their choice on the system or DHSC instructs NHSE to no longer run the service.		
How long do you intend to keep the information?	National Data Opt-Out will 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.		
What plans are in place for how the information will be retained/archived/transferred or disposed of, should this new/revised function stop?	Should the service no longer be required, the opt-out preferences will be anonymised or deleted in line with the NHS Records Management Code of Practice 2021.		
<b>Sharing Data – Tick as appropriate and provide details or leave blank if not applicable</b>			<b>IG Use Only</b>
Data is being sent or stored outside the UK	<input type="checkbox"/>		
Secure encrypted email is being used to transfer the information	<input type="checkbox"/>		
Secure electronic transfer is being used to transfer the information	<input checked="" type="checkbox"/>	MESH.	
Information is being shared with other organisations	<input checked="" type="checkbox"/>	NHS England.	

Data linkage – Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Data is being pulled together from different places, linked and/or cross-referenced	<input type="checkbox"/>		
As a result of linking data, it will be possible to identify individuals that were not identifiable from the original dataset	<input type="checkbox"/>		
Data Storage – Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Physical storage	<input type="checkbox"/>		
Local organisation servers	<input checked="" type="checkbox"/>		
Cloud Storage	<input checked="" type="checkbox"/>		
Other	<input type="checkbox"/>		
How will you ensure that information is safe and secure, when accessed, at rest and in transit? Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Encryption	<input checked="" type="checkbox"/>		
Password Protection	<input type="checkbox"/>		
Role Based Access Controls (RBAC)	<input checked="" type="checkbox"/>		
Restricted physical access	<input type="checkbox"/>		
Business continuity plans	<input checked="" type="checkbox"/>		
Secure policies (embed these)	<input type="checkbox"/>		
Other	<input type="checkbox"/>		
What will happen to the data at the end of the project? Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Secure destruction (i.e., shredding paper records or wiping hard drives with evidence cert of destruction)	<input checked="" type="checkbox"/>		
Permanent preservation by transferring to a Place of Deposit run by the National Archives	<input type="checkbox"/>		
Transfer to another organisation	<input type="checkbox"/>		
Extension to retention period	<input type="checkbox"/>		

It will be anonymised and kept	<input type="checkbox"/>		
The controller(s) will manage as it is held by them	<input checked="" type="checkbox"/>		
Other	<input type="checkbox"/>		

#### Section 4: Rights of Individuals – How are the rights of individuals complied with (where they apply)?

<b>The right to be informed about the collection and use of personal data - Tick as appropriate and provide details or leave blank if not applicable</b>			<b>IG Use Only</b>
Privacy Notice	<input checked="" type="checkbox"/>	The practices advertise the 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.	
Information Leaflets	<input type="checkbox"/>		
Posters	<input type="checkbox"/>		
Emails	<input type="checkbox"/>		
Texts	<input type="checkbox"/>		
Social Media Campaign	<input type="checkbox"/>		
Other	<input type="checkbox"/>		
Not applicable	<input type="checkbox"/>		
<b>The right of access – Tick as appropriate</b>			<b>IG Use Only</b>
Details all information used and the right to receive a copy of their personal information – this is commonly referred to as a ‘subject access request’	<input checked="" type="checkbox"/>	This right applies to all legal basis	
<b>The right of rectification – Tick as appropriate</b>			<b>IG Use Only</b>
Right to have inaccurate personal data rectified or completed if incomplete.	<input checked="" type="checkbox"/>	This right applies to all legal basis	
<b>The Right of Erasure – Tick as appropriate</b>			<b>IG Use Only</b>

Right to have personal information erased	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Only applies if: The information is no longer necessary for the purpose it was collected for The information is processed for direct marketing purposes and objection made The information is being processed unlawfully If consent and contract are the legal basis Assessed on a case-by-case basis	
<b>The Right of Restriction – Tick as appropriate</b>			<b>IG Use Only</b>
Right to limit how their personal information is used	<input checked="" type="checkbox"/> <input type="checkbox"/>	Only applies if: Information is inaccurate Information is being processed unlawfully	
<b>The Right to Data Portability – Tick as appropriate</b>			<b>IG Use Only</b>
Right to obtain and re-use their personal information	<input type="checkbox"/>	Only applies if consent or contract are the legal basis or when carrying out the processing by automated means	
<b>The Right to Object – Tick as appropriate</b>			<b>IG Use Only</b>
Right to object to the use and sharing of personal information	<input type="checkbox"/>	Only applies if consent is the legal basis	

## Section 5: Access and Reporting

<b>Access – Tick as appropriate and provide details or leave blank if not applicable</b>			<b>IG Use Only</b>
No access requirement	<input type="checkbox"/>		
Internal access requirement <i>(tell us who will be creating the accounts)</i>	<input checked="" type="checkbox"/>	Authorised GP Practice staff only.	
External access requirement <i>(describe authorisation process and who will be creating the accounts)</i>	<input type="checkbox"/>		
<b>Reporting – Tick as appropriate and provide details or leave blank if not applicable</b>			<b>IG Use Only</b>
New reporting requirements	<input type="checkbox"/>		
Additional reporting requirements	<input type="checkbox"/>		

No reporting requirements	<input checked="" type="checkbox"/>		
Reports will be run <i>(tell us who will run them, the types of reports, who will receive them and where published (if applicable))</i>	<input type="checkbox"/>		
The reports will be person-identified	<input type="checkbox"/>		
The reports will be pseudonymised	<input type="checkbox"/>		
The reports will be anonymised	<input type="checkbox"/>		
Plans are in place in relation to the internal reporting of a personal data breach <i>(tell us what the plans are)</i>	<input type="checkbox"/>	As per Trust policy.	
Plans are in place in relation to the notification of data subjects should there be a personal data breach <i>(tell us what the plans are)</i>	<input type="checkbox"/>	As per Trust policy.	

## Section 6: Business Continuity Planning

Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Personal data will be restored in a timely manner in the event of a physical or technical incident <i>(tell us how)</i>	<input checked="" type="checkbox"/>	As per Business Continuity/Disaster Recovery plans.	

## Section 7: Direct Marketing<sup>5</sup>

Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Personal data will be processed for direct marketing purposes	<input type="checkbox"/>		

## Section 8: Automated Processing<sup>6</sup>

Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
The processing will result in a decision being made about the data subject solely because of automated processing (including profiling <sup>7</sup> )?	<input type="checkbox"/>		

<sup>5</sup> Direct Marketing is 'the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals' – all promotional materials fall within this definition, including material promoting the aims of not-for-profit organisations

<sup>6</sup> Examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention

<sup>7</sup> 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

The decision is necessary for entering into or performance of a contract between the data subject and a controller	<input type="checkbox"/>		
The decision is authorised by the law	<input type="checkbox"/>		
The decision is based on the data subject's explicit consent	<input type="checkbox"/>		

## Section 9: Complying with Privacy Laws

<b>Privacy and Electronic Communications Regulation 2003 (amended 2019) PECR<sup>8</sup> - Tick as appropriate and provide details or leave blank if not applicable</b>			<b>IG Use Only</b>
This involves electronic marketing messages (by phone, email or text), cookies or providing electronic communications to the public	<input type="checkbox"/>		
<b>Human Rights Act (HRA) (Article 8)<sup>9</sup> – Tick as appropriate and provide details or leave blank if not applicable</b>			<b>IG Use Only</b>
The HRA considerations are not covered by this DPIA	<input type="checkbox"/>		
<b>Common Law Duty of Confidentiality<sup>10</sup> - Tick as appropriate and provide details or leave blank if not applicable</b>			<b>IG Use Only</b>
The project or service ensures compliance with the common law duty of confidentiality <i>(tell us how)</i>	<input checked="" type="checkbox"/>	All staff employed by the GP Practices, 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 that staff understand that whenever they handle, process and share personal information, they do so within strict codes of confidentiality integral to their day to day activities and must not disclose any information without the correct legal basis being applied.	

<sup>8</sup> UKGDPR sits alongside the PECR. PECR rules apply and use the UK GDPR standard of consent ([Consent | ICO](#)). For more information: [Guide to Privacy and Electronic Communications Regulations | ICO](#)

<sup>9</sup> Article 8: Right to Privacy – Everyone has the right to respect for their private and family life, their home and their correspondence

<sup>10</sup> In common law, there is a duty of confidentiality which means that when a patient/service user shares information in confidence, it must not be disclosed without some form of legal authority or justification. In practice, this usually means that the information cannot be disclosed without that person's consent

Transparency – Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
The existing Privacy Notices need to change <i>(tell us what changes are required)</i>	<input type="checkbox"/>		

## Section 10: Information Security

Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
There are security by design measures in place	<input checked="" type="checkbox"/>	The NHS 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 low.	
Technical configuration information (tell us about it)	<input type="checkbox"/>		
There are technical concerns that warrant further follow up	<input type="checkbox"/>		
This technology or similar is already in use in the Trust	<input type="checkbox"/>		
This is new technology which shares a commonly recognised platform eg O365, SharePoint	<input type="checkbox"/>		
Formal training is required before access is granted	<input type="checkbox"/>		
There are software, hardware and information assets are associated with this project or service	<input checked="" type="checkbox"/>	<p><b><u>Software Assets</u></b>  GP System - EMIS  MESH (if required as a back up to EMIS enabled functionality to set opt-out preferences) NHS Spine</p> <p><b><u>Hardware Assets</u></b>  Practice desktop PCs/laptops/any device with capability to connect to the internet</p> <p><b><u>Information Assets</u></b>  DPIA  National Data Opt-Out Policy  Privacy notices - compliance statement within the privacy notice. Opt-Out  Resources produced by NHS Digital</p>	

There is an Information Asset Owner <sup>11</sup>	✓	NHS England	
---	---	-------------	--

### Section 11: Review

Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Post-implementation checks will be carried out	<input type="checkbox"/>		

### Section 12: Audits

Tick as appropriate and provide details or leave blank if not applicable			IG Use Only
Ongoing maintenance will be assessed	<input type="checkbox"/>		
Regular audits will be required	<input type="checkbox"/>		

---

<sup>11</sup> Each information asset will have an Information Asset Owner. The information asset includes the records associated with the operation of the business function. Key decisions about the management of information will be made by the IAO. This includes records related to the asset and management of information risks pertaining to the asset. The IAO also ensures that the Information Asset Assistant, where appointed, carries out their duties to ensure that records are managed in line with guidance and policy.

## Risk Matrix

Risk Description	Inherent Risk Rating (AxB=C)			*Options for avoiding or mitigating this risk	Residual Risk Rating (AxB=C)		
	A = Potential Severity (1-5)	B = Likelihood (1-5)	Risk Rating (AxB)=C		A = Potential Severity (1-5)	B = Likelihood (1-5)	Risk Rating (AxB)=C
There is a risk that data could be subject to a cyber-attack.	3	3	9	Spine service management and information security plan. Annual penetration tests run by the Spine services team. Access and controls applied as if this was clinical data.	3	2	6
Unauthorised access or loss	2	2	4	Existing spine access controls. NHSE policies and procedures on access to data. NHS number data is extracted and applied automatically with no human intervention. NHSE terms and conditions for staff. Potential 'value' of opt-out data is considered low.	2	1	3
There is a risk that information assets are unavailable.	4	1	4	Spine target of 99.9% availability. Spine service management and information security plan.	3	1	3
There is a risk that cloud hosted solutions could suffer data loss and cyber-attack.	4	2	8	Only transient data stored on the Cloud. Cloud servers are hosted in the EEA.	3	2	6
There is a risk that data is stored by analytics and survey tools.	2	1	2	User 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.	2	1	2
There is a risk that the legal basis for processing is not established.	4	2	8	Directions from DHSC providing the legal basis for processing. Minimum audit data required for processing is stored. Clear privacy information ensures 'no surprises'.	3	1	3

	Rating
High	15-25
Significant	8-12
Medium	4-6
Low	1-3

The residual risk rating for this processing is classified as medium/low.

<b>DPIA Review and Approval Log</b>			
<b>Data Protection Officer Review</b>	Sahra Smith	<b>Date</b>	Click or tap to enter a date.
<b>Senior Information Risk Owner Approval (if applicable)</b>	Elizabeth Mellor	<b>Date</b>	08/08/2024
<b>Caldicott Guardian Approval</b>	Dennis Okolo	<b>Date</b>	22/08/2024
<b>Caldicott Guardian Signed Approval (if required)</b>	<INSERT SIGNATURE HERE>	<b>Date</b>	Click or tap to enter a date.