Data Protection Impact Assessment – GPES Data for Consented Research

Document filename:	DPIA for GPES Data for Consented Research	
Directorate / Programme	**Transformation / Data & Analytics**	
Document Reference	IAR reference 5810	
Information Asset Owner	Michael Chapman	Version 1.4
Author	**REDACTED**	

Document Management

Revision History

Version	Date	Summary of Changes
0.1	01/03/2025	Initial draft of document
0.2	25/04/2025	Amendments made to legal basis for disclosure and NDOO
0.3	16/06/2025	Further amendments made following review by DPO.
1.1.	09/07/2025	Additional risks added
1.2	15/10/2025	Redactions applied
1.3	18/11/2025	Minor edits
1.4	05/02/2026	Final review and updates made

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Redacted	IG Lead	17 Apr 2025	V0.1
Redacted	Deputy Director of IG Delivery (Digital and Operations) (2nd Line)	25 Apr 2025 16/07/2025	V0.1 V1.1
Redacted	IG Lead	25 Apr 2025	V0.1
Michael Chapman	Director of Data Access and Partnerships /IAO	6 Feb 2026	V1.4
Redacted	Head of NHS DigiTrials	15 Apr 2025	V0.1
Arjun Dhillon	Chief Medical Information Officer/Deputy Caldicott Guardian	14 May 2025	V0.2
Redacted	Assistant Deputy Director/Deputy Data Protection Officer	14 May 2025	V0.2
Jackie Gray	Director of Privacy and Information Governance	5 February 2026	V1.3
Redacted	IG Lead	6 February 2026	V1.4
Redacted	IG Lead	6 February 2026	V1.4

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
Michael Chapman	Director of Data Access and Partnerships / IAO	6 February 2026	V1.4

Jackie Gray	Director of Privacy and Information Governance	6 February 2026	V1.4

Document Control:

The controlled copy of this document is maintained in the NHS England corporate network. 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

1. Purpose of this document

A Data Protection Impact Assessment (DPIA) is a useful tool to help NHS England demonstrate how it complies with data protection law. The General Data Protection Regulation (GDPR) requires a Data Protection Impact Assessment (DPIA) to be completed by a controller where its processing of personal data is considered to be a high risk to the rights and freedoms of individuals. In particular GDPR requires a DPIA to be carried out where there is processing of personal data relating to health on a large scale.

The collection, processing and sharing by NHS England of this Collected Data is considered to require a DPIA to be carried out by NHS England. NHS England has therefore prepared this document as its DPIA to satisfy its own compliance requirements as a controller of the General Practice Data for Consented Research dataset. By completing this DPIA NHS England has systematically analysed its processing to demonstrate it will comply with data protection law and in doing so identify and minimise data protection risks.

2. Background

From 1 February 2023, NHS England has assumed responsibility for all activities previously undertaken by NHS Digital. This includes running the vital national IT systems which support health and adult social care, as well as the collection, analysis, publication, and dissemination of data generated by health and social care services. The statutory functions of NHS Digital transferred to NHS England under the Health and Social Care Information Centre (Transfer of Functions, Abolition and Transitional Provisions) Regulations 2023.

The Health and Social Care Act 2012 gives NHS England statutory powers, under section 259(1)(a), to require data from health or social care bodies, or organisations that provide publicly funded health or adult social care in England, that it considers necessary or expedient to have to carry out its functions under chapter 9 of the Health and Social Care Act 2012. This includes where it has been directed to establish an information system by the Secretary of State for Health and Social Care.

NHS Digital (now NHS England) was originally requested by representatives of the GP Profession to collect data from general practices in England for COVID-19 pandemic planning and research purposes: GPES Data for Pandemic Planning and Research (COVID-19) – (GDPPR). This was needed to respond to the intense demand for General Practice data to be shared in support of vital planning and research for COVID-19 purposes, and to relieve the growing burden and responsibility on general practices.

Although the pandemic is over, millions of people participate in research studies relating to health or where health is a relevant factor. Many of these studies have the Explicit Consent of participants to use routinely collected healthcare data to follow up the participants in an efficient and cost-effective fashion. Both the recent Sudlow Report[1] and the government's announcement of The Health Data Research Service[2] set out a much bigger ambition for the conduct of research in England, and the 10-year plan for the NHS echoes sentiments on

[1] Sudlow, CLM (2024). Uniting the UK's Health Data: A Huge Opportunity for Society.

https://doi.org/10.5281/zenodo.13353747

[2] https://www.gov.uk/government/news/prime-minister-turbocharges-medical-research

expanding research participation with the use of NHS data. The coded data held in the GP record is a rich source of information about health and for some conditions it may be the only place where a diagnosis or risk factor is recorded. In other cases it can complement other sources of healthcare data to give a more complete picture and avoid biases. Therefore, there remains a need to provide research studies with access to this data and relieve the burden on GPs, hence the re-collecting of GDPPR for consented studies.

The GPES Data for Consented Research Directions 2026 will enable provision of GP data to Approved Research Studies where participant consent, parental consent or consultee support (as established by virtue of s30-33 of the Mental Capacity Act 2005) is in place. This will be achieved by re-using the existing GPES (GP Extraction Service) Data for Pandemic Planning and Research (GDPPR) dataset, originally collected under the COVID-19 Public Health Directions 2020. Data will be made available to approved studies via the Data Access Request Service (DARS) through dissemination of linked extracts for the purposes of analysis and research aligned to an approved Data Sharing Agreement (DSA). DARS examine all requests, determine approval and specify the appropriate route to view / access the data and, when required, the examination includes scrutiny from the Advisory Group for Data (AGD).To be approved to receive this data, studies will also be required to meet a range of criteria as set out in the Requirements Specification, including that:

a. Consent materials clearly cover use of GP data for the proposed research and consent management processes (including management of withdrawal) are robust, have been audited by NHS England, assured by the Consent for Research Assurance Group (CRAG) and any priority recommendations are addressed.

b. Where applicable, the organisation has achieved Standards Met (or Partially Met where this is the required DARS standard) for the relevant assertions under the Data Security and Protection Toolkit.

c. If patient data is to be made available to other organisations under a sub-licence from NHS England, then access is only through a secure data environment (SDE) which the study has assured complies with the Department of Health and Social Care (DHSC) policy requirements and NHS England's Cyber Security team have assured certain agreed SDE security requirements are in place. In the longer term, the SDE must meet accreditation standards once introduced.

d. Data may only be accessed from the UK or countries permitted by NHS England under the relevant data sharing agreement following assurance by NHS England on UK GDPR compliance processes for overseas transfers. If patient data is to be made available to other organisations under a sub-licence from NHS England, then the study has a publicly accessible data uses register that details all the projects using NHS England data.

e. There are ongoing communications with research participants about how their data is used, including communications on the proposed sharing of GP data by NHS England with the research study before sharing commences

Any dissemination of participant data will be subject to a research study:

- applying to the NHS England Data Access Request Service (DARS);
- demonstrating to NHS England's reasonable satisfaction that they meet the criteria laid out in the Requirements Specification and other Access Criteria published by NHS England;
- entering into and complying with a DARS data sharing agreement (DSA);

- permitting NHS England to undertake audits in relation to the study's compliance with the DSA, including its compliance with the criteria set out in the Requirements Specification.

Data shared with Approved Research Studies under a DSA will be included in NHS England's Data Uses Registers.

3. Consultation with Stakeholders

NHS England has a requirement under section 258 of the Health and Social Care Act 2012, to ensure consultation has occurred with at least the following persons and groups:

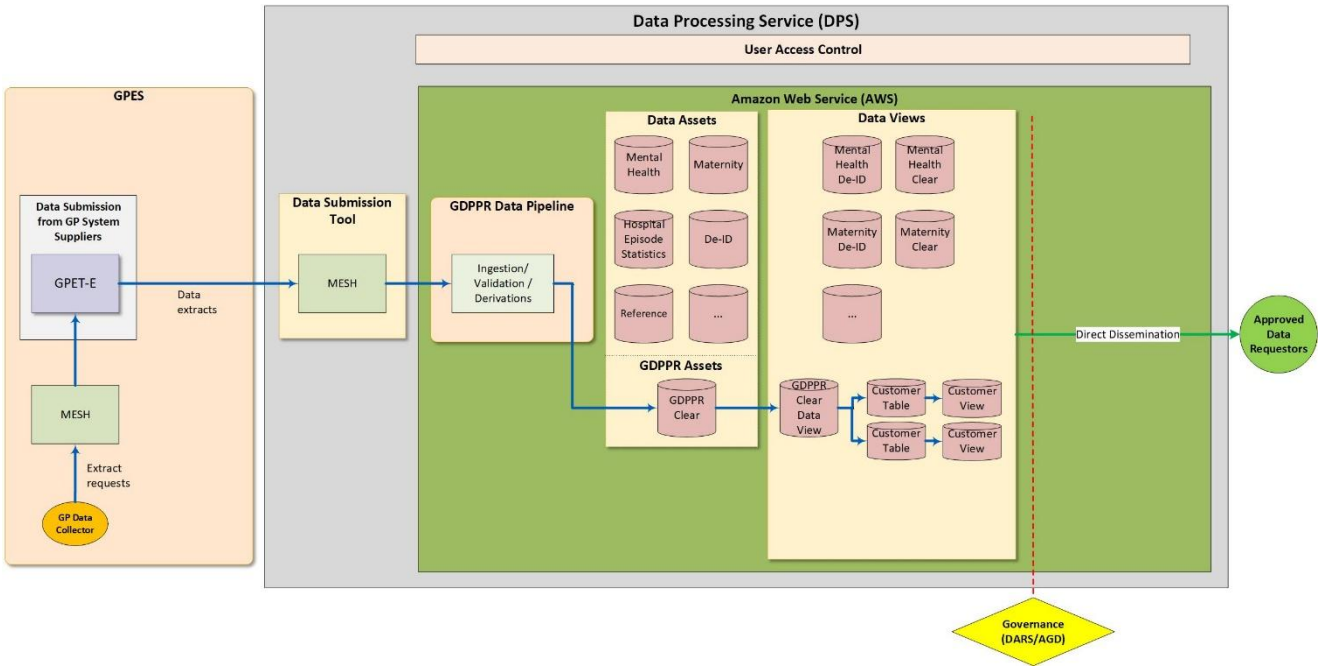
- The person who gave the direction or made the request,
- Representatives of other persons considered likely to use the information to which the direction or request relates,
- Representatives of persons from whom any information will be collected,
- Other persons considered appropriate.

In developing this service, the Department of Health and Social Care and NHS England have consulted the following stakeholders:

- The GP profession as represented by the British Medical Association (BMA) and Royal College of General Practitioners (RCGP), both through the Joint GP IT Committee and separate engagement
- Major consented research studies: Genomics England, Our Future Health, and UK Biobank
- Department of Health and Social Care
- The Association of Medical Research Charities
- Health Data Research UK
- Patient representative groups: useMYdata, Patients Association and National Voices
- MedConfidential
- The Information Commissioner's Office
- The National Data Guardian for Health & Social Care
- The Health Research Authority.

NHS England has also sought advice from its Advisory Group for Data (AGD).

4. Data Flow Diagram



NHS England will not collect any new data. It will access the data already collected as set out the GP Data for Pandemic Planning and Research (GDPPR) data specification and described in that DPIA.

The table below summarises the end-to-end flow from GP System Suppliers (GPSS) to the data being made available to end-users by NHS England via the Data Processing Services (DPS).

Category and Description of Processing	Entity Involved	Types of Personal Data Processed	What are the Data Processing and Security Arrangements
Stage 1: GP IT System Suppliers extract data to NHS England	Data Controller: GP Practice Data Processor: GP System Suppliers	Identifiable patient data	Data are held in GP patient record systems which meet national standards for security under relevant GP IT System contracts. Identifiable patient data will be extracted via the General Practice Extraction Tool - Extraction (GPET-E) within GPES. Exceptions process: In the event that the extract process fails, the GP system supplier will detect this and stop the process, thus preventing the data being transferred to NHS England.
Stage 2: GP IT System Suppliers provide data to NHS England	Data Controller: GP Practice and NHS England Data Processor:	Identifiable patient data	Data will be transferred to NHS England through an approved secure method of the Message Exchange for Social Care and Health (MESH). Exceptions process:

	GP System Suppliers		In the event that the transfer of data to NHS England fails, then the transfer will be repeated
Stage 3: NHS England receives data into the Data Processing Service	Data Controller: NHS England	Identifiable patient data	Data are processed in Data Processing Service to verify completeness and accuracy of data. Exceptions process: In the event that completeness and validation checks fail, then the cause will be investigated and, when resolved, the process will be restarted from stage 1 with the regeneration of the data extract.
Stage 4: Data is made available to end users	Data Controller: NHS England	Identifiable patient data	Users can receive and analyse the re-identified data, as per their authorisation via the DARS process. Exceptions process: In the event that a user receives data that they have not been authorised to access via the DARS process, NHS England investigates and reports a potential data breach through the appropriate channels.

5. Purpose of the processing

1. What is intended to be done with the personal data collected / used / processed / stored during this project?

The data collected and shared will be used by research studies consistent with the Explicit Consent given by participants or where parental consent or consultee support is in place and where those studies are approved to make use of the data.

All requests by organisations to access record level data from this collection will initially be reviewed by NHS England to determine their ability to meet the conditions set out in the Requirements Specification, any prioritisation based on capacity and advise on timelines. NHS England will then seek assurance, including through audit and review of materials provided by studies, that they meet the conditions. Data applicants will need to demonstrate they have a lawful basis to access and process the data for the required purposes. NHS England will seek Advisory Group for Data (AGD) advice on this. The request will then be presented to the Consent for Research Assurance Group (CRAG), which acts as an authoritative arbitrator, providing independent assurance that consented research studies are obtaining, recording and updating consents through robust and compliant processes that NHS England has also assured.

Data to be shared by NHS England will also be subject to data minimisation rules, restricting the data shared to that which may be reasonably expected to be required for the approved purpose. Data shared will be restricted to participants in the study. Additionally, not all detail on an individual need be shared. For example, if a research study is considering a particular disease, then only data relating directly to that study would be shared.

2. What will the intended results be, i.e. likely results for a GP Practice, impact (positive and negative, as applicable) on individuals concerned or (where applicable) other parties involved?

The intended results are to:

a. Meet patients' requests by sharing coded data from their GP records for research with specific Approved Research Studies; and

b. Unburden GPs from the workload and liability of managing data requests and data extractions at practice level.

Millions of people resident in England participate in research studies relating to their health or where health is a relevant factor. Many of these studies have the Explicit Consent of participants to use routinely collected healthcare data to follow up the participants in an efficient and cost-effective fashion. However, most patients' requests for their GP record to be shared are currently unmet.

Currently studies must establish individual agreements with GP practices to access data held about participants. This is burdensome for both research studies and GPs, who are not resourced to conduct the detailed review needed to ensure that requests from individual studies are legitimate.

3. What will be the benefits to the individuals concerned or (where applicable) other parties involved (including GP Practices) and to society?

Participants in research studies will benefit as data that they have agreed to share with research studies will be provided and used in line with the consent.

GP Practices will avoid the additional workload and potential liability of managing data sharing with individual research studies.

Research studies and – where those studies act as resources for others, the researchers who access data – will benefit from more comprehensive information about the health of participants, allowing them to study a wider range of diseases and avoiding potential biases if information held in GP records is excluded.

Individuals and society will ultimately benefit from improved treatments developed as a result of research conducted in these and other studies.

6. Description of the Processing

Nature and scope of the processing:

The source of the data is as described in the DPIA for the existing GDPPR data collection and is data already collected by NHS England for COVID-19 purposes under the COVID-19 Public Health Directions 2020. .

The data already collected and to be accessed by NHS England for consented research purposes consists of patient demographic information and coded medical information (as per the existing business rules for GDPPR) that are extracted from GP practices on a monthly basis by GPES as follows:

- Where patients register at a new practice

- Where journals[3] are added
- Journals are added and removed in between reporting periods
- Patients have died

Extracts / updates will not be collected where:

- Only changes made are in the patient section of the record.
- Only journals are removed.
- Only contents of journals are changed.
- Patients are deleted from practice registers.

Patients registered at a new practice one month before the reporting period end date until they have any relevant codes recorded within their new practice

GP System Suppliers extract data already held in GP Practice patient record systems and transfer this data to NHS England using the established General Practice Extraction Service (GPES) tool. The data provided will therefore be data which GPs have already obtained from patients and other third parties, including other healthcare professionals, for the purposes of providing healthcare services to patients. The data is not collected directly from the individuals themselves.

Description of the processing to be carried out:

[3] A 'journal' describes the coded record entries that make up a patient record for example a diagnosis of asthma, measurements such as blood pressure values or medications prescribed to the patient.

No	Compliance Requirement	Question	Answer	Risks (To be mitigated as set out in Section 19):
1	Nature of Processing Compliance with Lawfulness, Fairness and Transparency Principle	Explain how personal data will be collected Will you be collecting it directly from individuals? Do you already have the personal data, and if so, where did you get it from? Did you obtain the personal data from another organisation?	The Directions will enable NHS England to use the same data collection that is already collected and in place for GDPPR. This means that no additional data will flow to NHS England for this purpose. The GP Practice collects data from patients via registration forms and through appointments and treating the patient. Reports and test results are received from other medical providers and health care professionals involved in the patient's care which are also included in the patient health record. The data shared with NHS England is a subset of data which the GP Practice already holds in the patient records systems. The required data is collected from General Practices' clinical IT systems via the General Practice Extraction Service (GPES). The extract is transferred to NHS England's Data Processing Services (DPS) platform via Message Exchange for Social Care and Health (MESH). Type 1 Objections are applied to the GDPPR dataset collected by NHS England under the COVID-19 Direction. Therefore, the data for those patients who have registered a Type 1 objection with their GP will not be collected under the Consented Research Direction either and will not be available to share with an Approved Research Study, even if Explicit Consent has been provided by or on behalf of those patients, for so long as a Type 1 Objection is in place.	Risk that more data than is necessary for NHS England's purposes will be shared by GP Practice. (GP-DPIA-004) Risk that there is insufficient transparency to data subjects of the processing of their personal data for the purposes of the Project. (GP-DPIA-003)

2	Nature of Processing Compliance with Purpose Limitation Principle	How will personal data be used?	The Collected Data may only be used by NHS England and by other organisations for the purposes set out in the GPES Data for Consented Research Directions 2026 and accompanying Requirements Specification. Virtual result sets (or data views) of the data will be developed and provided where DARS-authorised requests permit a data file for dissemination, NHS England will use the customer-specific view to produce the data file for release via the normal SEFT and MESH processes.	Risk that Collected Data is used for purposes other than as specified in the Direction. (GP-DPIA-09) Risk that more data than is necessary for the approved purposes will be processed by NHS England. (GP-DPIA-004) Risk that more data than is necessary for third-party organisations' purposes will be processed by that organisation (GP-DPIA-009)
3	Nature of Processing Compliance with Storage Limitation Principle	Explain how personal data will be stored, e.g. On which IT platform? In hard copy? Third party cloud storage? For how long?	The Data Provision Notice and the GPES business rules provided to suppliers set out the scope of the collection. The GP IT System Suppliers develop the extract in accordance with the Business Rules. GPES is used to schedule and manage the collection and onward processing of the data into DPS. GPES is an established mechanism to schedule, extract and deliver GP Practice data from GP system supplier clinical systems. For the purposes of this collection, it is made up of three key components: DPS is the platform where the data will be processed and stored. NHS England uses Amazon Web Services (AWS) to host the data located within the UK, consequently AWS is a data processor for all data stored on DPS and NHS England has GDPR Article 28(3) compliant contracts in place with AWS. See Appendix C in the DPIA for GDPPR for more detail on security.	Breach of security resulting in unauthorised disclosure of personal data. (GP-DPIA-006)

			Data will be retained in accordance with the records management policy of NHS England. NHS England will retain the data collected for the following purposes: To make it available to approved organisations who continue to require it for approved research purposes and who have a legal basis to process it. For internal audit and legal record keeping purposes in relation to the data NHS England itself has analysed under the GPES Data for Consented Research Directions 2026 and in relation to the data disseminated to third parties.	
4	Nature of Processing Compliance with Integrity and Confidentiality Principle	Who can access the information collected during this project? (including any other third parties etc.?)	**External Parties** All requests to access the information will be made to NHS England who will be responsible for assessing and fulfilling the applications; these applications will only be successful if they pass the appropriate ethical, legal and Information Governance requirements. This is to ensure that data is only shared where it is secure, lawful and appropriate to do so. NHS England will do this through DARS (with advice from AGD). Data recipients will need to demonstrate they have a lawful basis to process the data for approved research purposes and NHS England will need to have a lawful basis to share the data with them for that purpose as determined through the DARS process. In addition, recipients will need to demonstrate that they meet the criteria set out in GPES data for Consented Research Requirements Specification.	Access arrangements are broader than necessary and result in increased risk that the Collected Data are used for unauthorised purposes. (GP-DPIA-007, GP-DPIA-014) Risk that Collected Data are used for purposes that are not expected. (GP-DPIA-09) Risk that Collected Data are subject to unauthorised access, or are lost, damaged or stolen (GP-DPIA-006)

			All requests to receive a data file must be approved through the DARS Data Sharing Agreement and will be serviced by NHS England using DPS to produce extract files for recipients of the data, which will be sent to the recipient using a secure mechanism such as MESH or SEFT. **Internal Parties** Only approved analysts in NHS England will have access to the Collected Data held in DPS for appropriate and necessary data management, preparation and analysis. Access to the data is strictly limited and subject to authorisation by the Information Asset Owner through NHS England's own Clear Data Access internal approval process. This process ensures that authorisation is only given to an individual for a time-limited period, where the access to the data is justified, and an appropriate legal basis for such processing is in place.	
5	Nature of Processing Compliance with Accountability Principle	Identify all external third parties that will have some involvement in the project (i.e. they may have access to, store or otherwise process the personal data)	The GP Practice system suppliers will perform the data extract using GPES. They are data processors for GPs and have been instructed by GPs to carry out the extract through GPs accepting the invitation to participate in the GDPPR collection through the Calculating Quality Reporting Service (CQRS). Data customers, with a legal basis to access the data approved by DARS (with AGD oversight). These will be approved research studies. Data processors acting on their behalf will be identified as part of any application process.	Risk that there are insufficient data protection controls around third parties who have access to the Collected Data. (GP-DPIA-007)

		Explain what their involvement / role will be in the project.	Amazon Web Services provides the IT Platform Infrastructure and is therefore data processor for data stored in DPS and the DAE. They have been appointed as a data processor by NHS England under contract which contains Article 28(3) compliant terms.	
6	Nature of Processing Compliance with Accountability Principle	Please identify any internal stakeholders this project has been discussed with Explain to which extent they are involved in the Project.	NHS England Data Protection Officer NHS England Data Access Request Service (DARS) NHS England Caldicott Guardian Information Asset Owner for GDPPR NHS England Cyber Security NHS England PTT Team NHS England Primary Care Team NHS England Assistant Director of Data Engineering NHS England Data Provisioning Team	Due to extent of involvement of key control areas within NHS England as identified here there is not considered to be a material residual risk arising from insufficient internal stakeholder involvement.
7	Nature of Processing Compliance with Storage Limitation Principle	Where geographically will the personal data be stored, or otherwise processed by any of the identified third parties? If the processing will involve	The geographical location of the data once transferred to NHS England is within the UK jurisdiction in the DPS Platform, which is hosted in the AWS cloud within the UK. All NHS England staff and contractors accessing the DPS will be doing so from within the UK. Where a research study applies to access the data, the DARS application specifically requests information about the Territory of Use for storage	Risk that Collected Data are transferred outside of the UK in breach of GDPR restricted transfer requirements due to ineffective monitoring of processing activity, including of disseminated data. (GP-DPIA-014)

		processing outside of the UK, where will the processing take place and what safeguards apply under Articles 45-49 GDPR?	and processing. The application process includes assuring the recipient's legal basis for processing within these territories, and in particular where such the territory of use is outside the UK. The Data Sharing Agreement with the Approved Research Study will limit data processing by the Approved Researcher to only those Territories assured and approved by NHS England.	
8	Nature of Processing Compliance with Storage Limitation Principle	When will personal data be deleted and how?	In line with NHS England records management policy, data will be kept for 8 years after last use for legal reasons to enable NHS England to exercise and defend its legal rights in relation to the data or any actions taken by NHS England e.g. analysis and dissemination (legal purposes). Data which has been disseminated will be held by the Data Recipient for the purposes and duration permitted under the relevant Data Sharing Agreement. This will be assessed as part of the DARS process.	The personal data is held for longer than necessary for the purposes set out in the General Practice Data for Consented Research Directions 2026 or other lawful authority considered in this DPIA. (GP-DPIA-012)
9	Accuracy Principle	How will the personal data be amended and kept up to date?	There will be monthly snapshots in time extractions via GPES. These snapshots will contain the full data set for any patient record that has had a SNOMED code added to their record since the previous extract, has newly registered at a GP practice or has died since the last extract, as outlined in section 6 of this DPIA. These patient records will be merged into the data set stored in DPS as part of the data ingestion pipeline.	Risk that the Collected Data is not up to date at the time of dissemination due to the time lags between the scheduled extractions and processing of the data into DPS. (GP-DPIA-008)

10	Scope of Processing	How many individuals are likely to be affected by the project?	Candidate patient records in the GDPPR collection are patients with active, current registrations at participating practices and deceased patients with a date of death on or after 1 November 2019. Records will not be included in the GDPRR dataset from patient records with a recorded dissent from secondary use of GP patient identifiable data, thereby respecting the Type 1 data opt-out. Further information is published on the care information choices webpage. Patient records will be included where they have coded record content that matches the codes defined by the Code Clusters applicable for the GDPPR dataset. It is estimated that approximately 54 million patients are included in the existing GPDPPR dataset under the COVID-19 Public Health Directions. However, only the specific subset of data required by Approved Research Studies from this dataset will be accessed and shared under the GPES Data for Consented Research Directions.	Risk that more data than is necessary for NHS England's purposes will be shared by GP Practice. (GP-DPIA-004)
11	Nature of Processing Compliance with Integrity and Confidentiality Principle	What security measures will you have in place to protect the personal data being processed?	**Security regarding transmission of data to and storage by NHS England** Data is extracted by GP systems suppliers using the GPES solution, which is an approved and established secure mechanism for extracting and delivering data. Once GPES collects the data, it is passed into a DPS AWS S3 bucket. This bucket enables security cleared role-specific access only. The data is then processed into a secure database,	Breach of security in the transmission of the data to NHS England and storage and other processing of the Collected Data which results in the unauthorised disclosure of personal data by NHS England. (GP-DPIA-006) Risk that data will be disseminated to Approved Research Studies that

			where it is kept separate from all other data sets stored within DPS. Backups of the data are supported by the DPS backup and recovery processes. DPS has a System Level Security Policy (SLSP) in place. **REDACTED** **Security regarding dissemination of data by NHS England** Data applicants will need to demonstrate through the DARS process that they have adequate security measures in place to protect the data where it is to be disseminated to them. Such security requirements are set out as part of the DARS application process and are documented on-line within the DARS section of the NHS England website. There are also specific security requirements that need to be met to satisfy the access criteria under the GP Data for Consented Cohorts Requirements Specification If patient data is to be made available to other organisations by an Approved Research Study under a sub-licence from NHS England, then such access is only permitted through a secure data environment (SDE) which the study has assured complies with the Department of Health Social Care (DHSC) policy requirements and NHS England Cyber Security team have assured certain agreed SDE security requirements are in place. In the longer term, the SDE must meet accreditation standards once introduced.	do not meet the required security standard expected by NHS England. (GP-DPIA-010)

			Under the terms of the Data Sharing Agreement and the Data Sharing Framework Contract NHS England can also carry out audits on compliance with the Access Criteria, including security requirements. DPST returns will also be monitored annually by NHS England.	
12	The Scope of Processing Compliance with Storage Limitation Principle	How long will the processing be taking place (i.e. for the duration of the project (provide number of weeks / months / years) and whether the processing will continue beyond the end of the project?)	The GDPPR dataset will be retained in accordance with the records management policy of NHS England and the Records Management Code of Practice for Health and Care Records 2021. NHS England will retain the data collected for 8 years from the date of last collection for the following purposes: • To make it available to Approved Research Studies who continue to require it for approved research purposes and who have a legal basis to process it • For internal audit and legal record keeping purposes in relation to the data NHS England itself has collected and shared under the General Practice Data for Consented Research Directions 2026	The personal data is held for longer than necessary for the purposes set out in the General Practice Data for Consented Research Directions 2026 or other lawful authority considered in this DPIA. (GP-DPIA-012)
13	The Nature of the Processing Compliance with Integrity and Confidentiality	Will data be anonymised, Pseudonymised, aggregated in non-personal information, etc?	The GDPPR dataset is identifiable data. The data that is shared from it with Approved Researchers will be in an identifiable form in order to meet the requirements of the research studies. Explicit Consent is given by participants for their personal data to be used for the purposes of these Approved Research Studies. Participant identifiers will be shared with NHS England by the Approved	

	and Data Minimisation Principle.	If so, please explain whether this is only externally or also internally within the organisation.	Research Studies to allow the extraction of GP data relating to their participants from the GDPPR dataset before being shared with the Approved Research Study, allowing them to link to other data already held by them about their participants.	

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

NHS England is directed by the Secretary of State, by virtue of s254 of the Health and Social Care Act 2012, to establish the information system for the collection of data for the purposes of operating the GP Data for Consented Research Service as set out in the Directions.

The Direction places a legal obligation upon NHS England to establish an information system for the purposes of delivery of this service. Therefore, NHS England's legal basis for processing under UKGDPR is Article 6(1)(c) – Legal Obligation. Further information regarding NHS England's legal bases for processing under UKGDPR is detailed in the transparency notice.

NHS England and the Secretary of State for Health and Social Care are Joint Controllers in relation to determining the purposes for which personal data is to be processed as set out in the GPES Data for Consented Research Directions 2026. NHS England is the sole organisation who processes information collected under the Directions and is fully responsible in law independently of the directing organisation for exercising its own statutory functions in relation to the collection and dissemination of information as set out in the Health and Social Care Act 2012

Actor	Role	Scope
Secretary of State for Health and Social Care (Secretary of State)	Joint Controller	The Secretary of State is a joint controller with NHS England in relation to determining the purposes for which personal data is processed under the Direction.
NHS England	Joint Controller and Independent Controller	NHS England is a joint controller with the Secretary of State in relation to determining the purposes for which personal data is processed under the Directions. It is the sole controller for the processing of personal data.

Information System - The Direction places a legal obligation upon NHS England to establish an information system for the purposes of delivery of the service and therefore NHS England is operating under:-

- Article 6(1)(c) of UKGDPR: as the processing is necessary for compliance with a legal obligation by virtue of complying with the Direction; and

- UK GDPR Article 9(2)(g) - substantial public interest, supplemented by DPA 2018 Schedule 1, Part 2, paragraph 6 - statutory and government purposes. NHS England may process what is necessary to enable it to comply with an enactment - that is, the direction or mandatory request issued under the 2012 Act.

Legal basis for disclosure

Statutory Basis & Common Law Duty of Confidence

Data obtained under the Direction will only be disseminated to Approved Research Studies approved to receive it and listed on the NHS England website. Approved Research Studies are able to apply to DARS and on approval, with the appropriate legal basis, have access to data obtained under the Direction. Any dissemination will be subject to the organisations applying to access the data having a lawful basis to process it, NHS England having a lawful basis to disclose it, successful applications being made to the NHS England DARS and the organisations entering into a data sharing agreement.

Where research studies have been approved, NHS England will use its discretionary powers under section 261 of the Health and Social Care Act 2012 and under any other statutory powers to disseminate data to Approved Research Studies. In most cases NHS England will share information only where the sharing conforms to the following conditions set out in s261 of the 2012 Act;

1. For patients who have provided consent: -if it considers that disseminating the information would be for the purposes connected with—

   the provision of health care or adult social care, or

   the promotion of health.

   (as per s261(1) & (1A) of the 2012 Act)

and

2. the information is in a form which identifies any individual to whom the information relates or enables the identity of such an individual to be ascertained and the individual has consented to the dissemination.

   (as per s261(2)(c) of the 2012 Act)

The common laws duty of confidence is met by the patient providing explicit consent

For patients where a consultee has provided advice to support the patient becoming a participant in the research:

- Organisations with research functions established by law, e.g. universities set up by legal charter etc

  Statutory basis: s261(5)(d), the organisation has functions established by law

  Duties of confidence: best interest advice provided under sections 30-33 of Mental Capacity Act 2005

- Organisations which do not have research functions established by law, but conducting research, there is no such provision in s261 therefore we rely upon our wider functions under the NHS Act 2006

  Statutory basis: s13(z)(3)(f) NHS Act 2006, NHS England disclosing data to meet its statutory functions to support research as per s13L of the NHS Act 2006

  Duties of confidence: best interest advice provided under section 30-33 of the Mental Capacity Act 2005

Data approved via the DARS agreements will be included in our Data Uses Registers

UK GDPR

Personal data will be processed under UK GDPR:

- Article 6(1)(e) - performance of task in the public interest or exercise of official authority, supplemented by DPA 2018 section 8(c) - processing that is necessary for the exercise of a function conferred on NHS England by enactment – that is the direction issued under section 254 of the 2012 Act.

- UK GDPR Article 9(2)(g) - substantial public interest, supplemented by DPA 2018 Schedule 1, Part 2, paragraph 6 - statutory and government purposes. NHS England may process what is necessary to enable it to comply with an enactment - that is, the direction issued under section 254 of the 2012 Act.

- UK GDPR Article 9(2)(j) - processing is necessary for scientific research purposes or statistical purposes in accordance with Article 89(1) supplemented by DPA 2018 Schedule 1, Part 1, paragraph 4.

8. Demonstrate the fairness of the processing

NHS England will only share patient data with an organisation conducting health related research where it can demonstrate that Explicit Consent has been obtained from participants. This includes where parental consent is given on behalf of a child (unless the principle of Gillick Competence is applied) and individuals lacking capacity, where consultees have given advice that the individual would wish to take part in the research if they were able to give consent themselves as defined in the Mental Capacity Act 2005. Participants (or parents/guardians and consultees) will have been provided with participant information detailing how their (or their child/the individual they are advising on behalf of) data will be obtained and further processed.

The data to be shared is minimised and is protected through technical controls including minimisation of data to those participants in the Approved Research Study only and, where appropriate, the selection of specific codes, and creation of derived fields.

The data is also shared with Approved Research Studies under a data sharing framework contract and agreement, which restrict the use of the data to that which is set out within the agreement. The agreement also only allows other data to be linked with the data where agreed within the DSA.

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

Detailed information regarding the GP Data for Consented Research Service has been made publicly available, including:

- A specific NHS England Transparency Notice has been drafted which provides details regarding how and why NHS England will process and use patients' personal data for the purposes of consented research including information about the rights available to individuals to exercise.

- An amendment referring to the GP Data for Consented Research Service has been made to the existing GDPPR GP Transparency Notice which can be used by GPs to provide updated transparency to their patients through publication on their website. This also provides full details including rights individuals have.

- A Data Provision Notice to GPs published on NHS England's website. This provides full details about the Service, including the purpose, benefits, legal basis and the form, manner and period of the data collection which underpins the Service. The Data Provision Notice is the formal notice that is issued to general practices ahead of the Service commencing to provide GP practices with notice of the re-use by NHS England of the GPDPPR dataset for the GP Data for Consented Research Service.

- Business Rules for the original GPDPPR dataset. These provide a detailed technical specification of the data items and structure of the dataset which is being used to deliver the GP Data for Consented Research Service and are available on the NHS England website here.

- Direction. The GPES Data for Consented Research Directions 2026 is published on the NHS England website and is referenced in the Data Provision Notice and Transparency Notices. This ensures that NHS England is transparent in showing the public what it has been directed to do

- Website content – a dedicated webpage provides information on the data collection.

- Consultation with groups that represent patients' and public interest in data including the Office of the National Data Guardian, useMYdata and the Information Commissioner's Office.

- Data Uses Register – details of all disseminations of data made by DARS under its data sharing agreements to Approved Research Studies will be published on its register of approved data releases. The identities of Approved Research Studies will also be published on the NHS England website

In addition, each research organisation is responsible for obtaining Explicit Consent from each participant (or consent alternatives where the participant is a child or consultee advice for a participant lacking capacity). This process requires participants (or

parent/guardian/consultee) to be fully informed of the research study and details of how personal data will be processed. Participants (or parent/guardian/consultee) will be provided with information sheets and consent forms which detail what data the research organisation will process about the individual.

One of the conditions of approval to become an Approved Research Study to receive data through the GP Data for Consented Research Service is also that Approved Research Studies contact their participants to tell them about receiving data form their GP health record from NHS England.

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

The following list of data items is already collected as part of the GDPPR datasets and will be processed for the purposes of the GP Data for Consented Research Service.

Data Categories Information relating to the individual's:	**Select as appropriate**	**Justify** There must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing. Is processing of this data **proportionate** to the aim of the processing? Explain why.
Personal Data		
Name	☒	Current data only. Forename and Surname will be provided by the GP system supplier. If the NHS Number field is empty then Forename is one of the fields that can be used by NHS England to match the patient data to its NHS Number.
Address	☒	Current data only. Address will be provided by the GP system supplier. If the NHS Number field is empty, then Address is one of the fields that can be used by NHS England to match the patient data to its NHS Number. Address or partial address also enables stratification by geographic locations where postcode is not sufficiently granular, and thus research into specific outbreaks of disease, incidence rates, association with deprivation and general epidemiological analysis.
Postcode	☒	Current data only. Postcode will be provided by the GP system supplier. Lower Layer Super Output (LSOA) will be derived from this value by NHS England to be used as a minimised alternative where possible. LSOA is also used as a deprivation index. Postcode enables stratification by geographic locations and thus research into specific outbreaks of disease, incidence rates, association with deprivation and general epidemiological analysis
DOB	☒	Current data only. Date of Birth will be provided by the GP system supplier. Year of Birth will be derived from this value by NHS England to be used as a minimised alternative where possible. DOB enables stratification by age, and general epidemiological analysis.
Sex	☒	Current data only. Sex will be provided by the GP system supplier. Sex enables stratification by this item and thus research into incidence rates, association with deprivation and general epidemiological analysis and potential inequalities (e.g. trends in disease prevalence for males).

Data Categories Information relating to the individual's:	**Select as appropriate**	**Justify** There must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing. Is processing of this data **proportionate** to the aim of the processing? Explain why.
Physical Description	☒	Current and the last 2 years of values relating to Physical Description as specified for relevant SNOMED codes in the business rules The Patient Record may contain clinical codes that could relate to the individual's physical description such as 'obese' where these occur within specified SNOMED codes.
General Identifier e.g. NHS No	☒	Current data only. NHS Number will be provided by the GP system supplier. Where the NHS Number field is blank, DPS may use other demographic details collected (e.g. surname) in combination in an attempt to find the related NHS Number if it is decided that there is a problem with missing NHS Numbers.
Date of Death	☒	Current data only. Date of Death will be provided by the GP system supplier. Date of Death enables establishment of cohorts of fatalities and general epidemiological analysis.
Special Category Personal Data The UK GDPR's Data Minimisation Principle states that personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Special Categories of Personal Data are particularly sensitive items of personal data, and the processing of such data is PROHIBITED unless one or more exemptions apply under Article 9 of the UK GDPR. There is a section below for you to explain what Article 9 exemption(s) will apply, however, for the purposes of this section, the Data Minimisation Principle requires you to adequately justify why it is necessary to process Special Categories of Personal Data taking into consideration of the objectives of the processing.		
Physical / Mental Health or Condition	☒	Current and the last 2 years of values relating to Physical/Health Condition as specified for relevant SNOMED codes in the business rules. The Patient Record may contain clinical codes that relate to the individual's physical and/or mental health/conditions such as 'depression' where these occur within specified SNOMED codes.
Sexual Life / Orientation	☒	Current and the last 2 years of values relating to Physical/Health Condition as specified for relevant SNOMED codes in the business rules. The Patient Record may contain clinical codes that relate to the individual's physical and/or mental health/conditions which reference a sexually transmitted infection (STI), human immunodeficiency virus (HIV), acquired immune deficiency syndrome (AIDS) or a gender related disorder, because the code occurs within relevant SNOMED codes in the business rules, e.g. these are codes relating to respiratory conditions or cancers which are relevant in the context of the approved research. Therefore, the extract does contain sensitive codes (171) which are listed in the SNOMED reference tables of codes relating to sensitive information.
Racial / Ethnic Origin	☒	The current value on the GP record and all historic values. Ethnicity will be provided by the GP system supplier. Ethnicity enables stratification by this item and thus research into incidence rates and potential inequalities (e.g. trends in disease prevalence for black and minority ethnic groups) and general epidemiological analysis.

How have you complied with the Data Minimisation Principle?

During the COVID-19 pandemic, NHS England (then NHS Digital) engaged with GP professional bodies, research organisations and GP IT System Suppliers to establish the minimum necessary data set to meet established and developing use cases, as set out in the Data Provisioning Notice and Business Rules. NHS England is using that dataset as a

source to extract relevant data only for the purposes of sharing it with Approved Researchers under the GP Data for Consented Research Service

This minimum necessary dataset includes:

• limitations where historic data is not required to meet uses due to its age:

- only current values for patient demographic data are collected (exception being Ethnicity where historic values are also collected);
- only historic values for the last two years for data relating to measurements, tests and interventions are collected;

• legally restricted codes for Gender Recognition and Human Fertilisation and Embryology are not collected as these codes are not included in the business rules issued to GP IT System Suppliers.

• 171 sensitive codes are collected, including codes which are listed in the 'Sexually Transmitted Disease' and the 'Gender Related' SNOMED reference tables of codes relating to sensitive information. The justification for collecting these codes is set out in the table above under the Data Item/Category of 'Sexual Life'. Any sensitive coding may only be disseminated as part of a data release including identifiers where the purpose justifies that release, and there is an appropriate legal basis. All sensitive codes are separated from standard codes within DPS to enable these to be handled appropriately.

It should be noted that the GPES tool only collects structured and clinically coded data (e.g. free text, images and documents are not collected).

All codes collected are listed in the GPES Data for Pandemic Planning and Research (GDPPR) data specification.

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

Data may be linked to other data held by NHS England at the request of Approved Research Studies or once disseminated linked to other data held by those Approved Research Studies for the approved purposes under the GPES Data for Consented Research Directions 2026. NHS England will only make the data available for approved research purposes when the criteria set out in the Requirements Specification are met and the purposes are consistent with the consent given by participants.

The agreement also only allows other data to be linked with the data where agreed within the DSA.

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

Requests for data will be managed through the existing DARS process, that is, an organisation will apply to DARS to be approved to receive the data as per the existing governance. Research studies will also be required to meet a range of criteria to use this

data under the terms of the Direction and its Requirement Specification, as listed in Section 2 of this document.

13. How long will the personal data be retained?

Data will be retained in accordance with the records management policy of NHS England and the Records Management Code of Practice for Health and Care Records 2021.

NHS England will retain the GPDPPR data already collected for the following purposes:

- To make it available to approved organisations who continue to require it for approved research purposes and who have a legal basis to process it
- For internal audit and legal record keeping purposes in relation to the data in the GPDPPR dataset that NHS England itself has accessed and shared under the General Practice Data for Consented Research Directions 2026 to enable NHS England to exercise and defend its legal rights in relation to the data or any actions taken by NHS England e.g. dissemination (legal purposes).

Data which has been disseminated will be held by the Data Recipient for the purposes and duration permitted under the relevant Data Sharing Agreement. This will be assessed as part of the DARS process.

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

Responsibility for data accuracy within patient records lies with the GP Practices as the source data controller. Where updates are made to GP records, these updates will be collected by NHS England as part of the next data collection of the GPDPPR dataset. The dataset used to deliver the GP Data for Consented Research Purposes by NHS England is therefore updated every month.

NHS England shall ensure the last date of the collection is clearly made known to the Approved Research Studies for data shared with them, to prevent misinterpretation of the data recency.

Data extraction and sharing frequency with Approved Research Studies will be reviewed based on study requirement and NHS England capacity to execute extractions from the GPDPPR dataset for sharing.

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

Individuals (data subjects) have the following rights under the GDPR:

- The right to be informed – Fair Processing information and Transparency Notice for NHS England and GPs have been developed by NHS England and made available prior to the GP Data for Consented Research Service commencing. In addition, each Approved Research Study is responsible for obtaining Explicit Consent from each participant (or consent alternatives where the participant is a child or consultee advice where a participant is lacking capacity). This process requires participants (or parent/guardian/consultee) to be fully informed of the research study and details of how personal data will be processed. Participants (or parent/guardian/consultee) will be provided with information sheets and consent forms which details what data the research organisation will process about the individual. Approved Research Studies will also inform their participants about receiving GP data from NHS England as a condition of their approval

- The right of access - An explanation about how an individual can request a copy of information that NHS England holds, including the GPES dataset, is published here. NHS England has established processes for handling Subject Access Requests through the Data Protection and Trust Team). NHS England has established that a patient record can be extracted and the explanatory textual description supplied for each of the SNOMED codes. Any patient can also request to view part of their medical records from the Practice either through the GP Practice system supplier or via the NHS App. Lastly patients can request access to information in their health records by making a Subject Access Request to the GP Practice. Information about how to make these requests should be available on GP Practice websites. To minimise the burden on GPs at this time patients are encouraged to register and use NHS App services which include access to medical records.

- The right to rectification - The right for individuals to request inaccurate personal data is rectified or completed if it is incomplete. Patients will need to contact their GP Practice to ensure that inaccurate data held on GP Practice IT systems is amended. As the Collected Data will be supplied to NHS England on a monthly basis, any updates to the patient record will be supplied regularly.

- The right to erasure – NHS England processes the personal data under Article 6(1)(c) of UKGDPR: as the processing is necessary for compliance with a legal obligation by virtue of complying with the Direction. As such, the right to erasure does not apply.

- The right to restrict processing - Where an individual contests the accuracy of their personal data NHS England will consider the request.

- The right to complain - Individuals who believe that their data is not being processed in accordance with the law can complain to the Information Commissioner's Office (ICO). They can also contact NHS England's Data Protection Officer (DPO) regarding NHS England data processing activity and the DPO of their general practice regarding GP data processing activity. Details for the NHS England DPO are contained on the NHS England website in the General Transparency Notice.

- The right to data portability - Is not applicable to this processing because under article 20 (3) the processing is being carried out in the exercise of official authority vested in the controller under Article 6(1)(c) legal obligation under the General Practice Data for Consented Research Directions 2026 or under Article 6(1)(e) public task.

- The right to object – This right is applicable to processing based on the lawful basis of public task. However, NHS England is processing the personal data under Article

6(1)(c) of UKGDPR: as the processing is necessary for compliance with a legal obligation by virtue of complying with the Direction. As such, the right to object does not apply.

- Patients that have registered a Type 1 objection with the GP Practice will not have their data shared with NHS England as this is one of the business rules agreed with the BMA and RCGP in relation to the GPDPPR dataset. This is made clear in the Transparency Notices. Patients can remove their Type 1 objection following local processes established by their GP practices.

- Patients who have registered a National Data Opt-Out can agree to take part in a specific research project by giving their Explicit Consent. This Direction and use of the data in the GDPPR dataset relates to patients participating in health research who have given Explicit Consent for their GP data to be processed for the purposes of the research study or where a consultee has provided advice and other safeguards within s30-33 of the Mental Capacity Act 2005 apply. As such, the National Data Opt-Out does not apply to data shared under the GP Data for Planning and Research Service.

- Rights in relation to automated decision making and profiling - no automated decision making or profiling is intended to take place as part of the GP Data for Planning and Research Service by NHS England.

What measures are in place to ensure NHS England's processors comply with GDPR and NHE England's instructions in relation to this project?

No processors of NHS England are actively involved in the processing carried out on behalf of NHS England to collect, analyse or disseminate the data. The Collected Data is stored in DPS which uses Amazon Web Services (AWS), a cloud service hosted in the UK. AWS is a data processor for all data stored on DPS and NHS England has a GDPR Article 28(3) compliant contract in place with AWS who have been appointed to provide the cloud services. Any changes in the instructions to AWS would be processed in accordance with the change control mechanisms under the contract.

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

Data is extracted by GP systems suppliers using the GPES solution, which is an approved and established secure mechanism for extracting and delivering data. Once GPES has collected the data, it passes into a DPS AWS S3 bucket. This bucket enables security cleared role-specific access only. The data is then processed into a secure database, where it is kept separate from all other data sets stored within DPS. Backups of the data are supported by the DPS backup and recovery processes. DPS has a System Level Security Policy (SLSP) in place.

REDACTED

Security regarding dissemination of data by NHS England

Data applicants will need to demonstrate through the DARS process that they have adequate security measures in place to protect the data where it is to be disseminated to them. Such security requirements are set out as part of the DARS application process and are documented on-line within the DARS section of the NHS England website. Specific security requirements to be met for the GP Data for Consented Research Service are set out in the Requirements Specification.

If patient data is to be made available by an Approved Research Study to other organisations under a sub-licence from NHS England, then access is only permitted through a secure data environment (SDE) which the study has assured complies with the Department of Health Social Care (DHSC) policy requirements and NHS England Cyber Security team have assured certain agreed SDE security requirements are in place. In the longer term, the SDE must meet accreditation standards once introduced

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

Data held and processed by NHS England to deliver the GP Data for Consented Research Service is stored in the UK and may only be accessed from the UK. In relation to data shared with Approved Research Study, processing outside of the UK will only be permitted in Territories where NHS England is assured that the Approved Research Study is complying with UK GDPR and where approval to process in those Territories is provided by NHS England under the relevant data sharing agreement.

18. Does the National Data Opt-Out apply to the processing?

Does the National Data Opt-Out apply? - No

The National Data Opt-Out (NDOO) allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment - for research and planning. When a patient has set an NDOO, organisations covered by the opt-out policy must make sure the patient's opt-out choice is respected.

However, If a patient has agreed to a specific use of data, after being fully informed, then the NDOO does not apply. Patients who have registered a National Data Opt-Out can agree to take part in a specific research project or clinical trial, by giving their Explicit Consent.

This Direction relates to patients participating in health research who have given Explicit Consent for their GP data to be processed for the purposes of the research study or where a consultee has provided advice and other safeguards within s30-33 of the Mental Capacity Act 2005 apply. As such, the national opt-out does not apply to the data shared under the GP Data for Consented Research Service.

• Identify and assess risks

Important: Any residual high risks (i.e. risks which remain high even after applying available mitigations, MUST be referred to the DPO for review before any processing takes place. Prior notification of such circumstances to the ICO may be required by law.

Please note that 'risks', in the context of this section, refer to risks to the data subjects.

To assess overall risk rating as 'low', 'medium' or 'high' risk for sections 18A and 18B below, consider the severity of impact and likelihood of harm (to data subjects) and, using the table below, determine the risk score. You can then use the key below to determine if the risk number corresponds to a 'low', 'medium' or 'high' risk. For example, a risk that is a 'reasonable possibility' and is likely to cause serious harm to the data subject will score 4 and will therefore be a 'high' risk.

Scoring key:

1 or 2 = LOW RISK 3 = MEDIUM RISK 4 or 5 = HIGH RISK

Severity of impact	Serious harm	3	4	5
	Some impact	2	3	4
	Minimal impact	1	2	3
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

19A: Risks Prior to Any Mitigations:

NHS England (NHSE) has a duty to manage data appropriately and share data legally, efficiently, effectively, transparently and in line with public expectation. All data sharing brings an element of risk. However, these risks must be balanced against NHS E's responsibilities to support research that benefits the health and social care of the citizen.

Risk reference:	Risk Type	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)
GP-DPIA-001	Confidentiality Fairness	Data Recipient Consent Process	There is a risk that Explicit Consent has not been obtained from participants to use data from their GP records.
GP-DPIA-002	Confidentiality Fairness	Data Recipient Consent Process	There is a risk that consent obtained from participants has not been maintained.
GP-DPIA-003	Transparency	Data Recipient Consent Process Transparency Materials	**Inadequate or no Transparency** Patients are not informed about how their personal data is being used through inadequate or lack of transparency material The risk to data subjects is that their personal data is processed in an unfair or unexpected way, potentially causing distress. This would breach the fairness principle 1 of GDPR and Articles 13 and 14. It could also result in data subjects not being aware of their data subject rights.
GP-DPIA-004	Minimisation	Data Provision Notice GP System Supplier GPES	**More data than is necessary for purposes specified in the COVID-19 Public Health Directions 2020 and GPES Data for Consented Research Directions 2026 are shared by GP Practices and Processed by NHS England.** Either because the data items were not all required or because the system for collection takes data items outside of the items covered by the DPNs including Restricted Data. The risk to data subjects is of distress caused by processing data about them they did not expect would be shared with or by NHS England.
GP-DPIA-005	**REDACTED**	**REDACTED**	**REDACTED**
GP-DPIA-006	**REDACTED**	**REDACTED**	**REDACTED**
GP-DPIA-007	**REDACTED**	**REDACTED**	**REDACTED**
GP-DPIA-008	Security	Data Access Request Service (DARS) - Data Dissemination	**Breach of security by NHS England in the dissemination of the Collected Data through making the incorrect data available through a DARS data file resulting in the unauthorised disclosure of personal data to third parties and a personal data breach.** The risk to data subjects is distress, anxiety and other harm to the rights and interests

GP-DPIA-009	Security	Data Access Request Service (DARS) - Data Dissemination	**Risk of unauthorised access of the Collected Data within NHS England resulting in the data being used for unauthorised purposes.** The risk to data subjects is that their personal data including special category data is processed by unauthorised third party resulting in distress, anxiety and other harm to the rights and interests of the data subject
GP-DPIA-010	Security	Data Access Request Service (DARS) - Data Dissemination	**Risk of data being disseminated to organisations that do not meet the required security standard expected by NHS England** The risk to data subjects is that their personal data including special category data is subject to a security breach by an Approved Research Study and disclosed to an unauthorised third party resulting in distress, anxiety and other harm to the rights and interests of the data subject
GP-DPIA-011	Purpose Limitation	Direction Transparency Materials	**The Collected Data are used for a purpose outside of what is defined in the GPES Data for Consented Research Directions 2026 by data recipients.** The risk to data subjects is that their data could be processed for purposes beyond those which they expected, and which were set out in the Transparency Notices provided by NHS England and GPs. This could cause the data subject to suffer distress and otherwise impact on their rights and interests including that their data is used for purposes that they might reasonably consider inappropriate or unethical.
GP-DPIA-012	Storage Limitation	Direction Records Management Data Recipient Consent Process	The personal data is processed for longer than necessary for the purposes set out in the General Practice Data for Consented Research Directions 2026 by (i) NHS England (ii) the data recipient Retaining and processing data for longer than is necessary will cause distress to data recipients.

GP-DPIA-013	Accuracy	GP System Supplier GPES	**Risk that inaccurate data is collected, analysed and disseminated to authorised organisations** Data is collected on a monthly basis. Due to the monthly extraction frequency, there is a risk that the data may not be up to date at the time of dissemination This could lead to inaccurate data being used for authorised purposes. As the data is being used for secondary use purposes it is unlikely that this will have an impact on the individual concerned.
GP-DPIA-014	Data Subject Rights	Data Access Request Service (DARS) - Data Dissemination Data Recipient Consent Process	**Risk that Collected Data is transferred outside of the UK to a jurisdiction which does not provide for sufficient protections of the rights of data subjects as required under GDPR** The risk to data subjects is that the data protection arrangements in the jurisdiction where processed are not as robust as in the UK and do not provide the same level of safeguards over their data or afford them the ability to exercise their data subject rights in the same way.
GP-DPIA-015	Policy	Type 1 Objections Policy	**Type 1 Objections are applied overriding participant consent** The consequences of excluding records with Type 1 Objections from the GPDPPR collection and overriding consent would cause data subjects distress. The risk to data subjects is that the Explicit Consent given to the research organisation for it to obtain GP data via NHS England does not override an existing Type 1 objection.
GP-DPIA-016	Policy	Breach of data minimisation if COVID-19 Directions revoked or GPDPPR collection is no longer required under those Directions	These Directions specify NHS England are to collect the GPDPPR dataset and are therefore not dependent on the COVID-19 Directions continuing. If the COVID19 Directions are revoked or the collection no longer required for COVID-19 purposes, NHS England would still be legally obliged to continue to collect the GDPPR data, however the data collection would contain records of patients who have not consented to their data being shared with Approved Researchers as well as those who have consented.

GP-DPIA-017	Accuracy	Risk that data is shared for a patient who is not a participant due to a mismatch with NHS number shared with NHSE by the approved research study with their participant	There is a risk that there is an error or a confusion that results in an NHS number being shared with NHSE that does not relate to a patient who has consented.
GP-DPIA-018	Security	Risk of security breach by Approved Research Studies associated with data being accessed by third party researchers from their SDE	There is a risk that third party access to data held by Approved Research Studies in their SDEs occurs which results in data being shared outside of SDEs in breach of the terms of the DSA with NHS England and/or in breach of UKGDPR

19B: Assessment of Risk / Residual Risk Assessment:

Against each risk you have identified, record the decision on risk, options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

Risk	**Which elements of the initiative give rise to privacy risks?**	**What is/are the potential or actual privacy risk(s)**	**Likelihood**	**Impact**	**RAG status**	**Decision on Risk:** Tolerate/Terminate/Treat/Transfer	**Proposed solution(s)/mitigating action(s) –** *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	**Likelihood**	**Impact**	**RAG status**	**Action**	**Target Date for completion**
GP-DPIA-001	Data Recipient Consent Process	There is a risk that Explicit Consent has not been obtained from participants to use data from their GP records.	Reasonable possibility	Some impact	3	Treat	A robust consent assurance will be undertaken and shared with CRAG to provide assurance that the consent given is compatible with the provision of GP data. Additionally, AGD will review consent materials when providing advice on a DARS application.	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-002	Data Recipient Consent Process	There is a risk that consent obtained from participants has not been maintained.	Reasonable possibility	Some impact	3	Treat	Every DARS application for GP data will be subject to a Consent Assurance Audit to ensure that the consent process is appropriately managed and maintained particularly in relation to processing withdrawals from the study. Audits will be carried out for all Approved Research Studies and shared with CRAG	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	*Proposed solution(s)/mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-003	Data Recipient Consent Process Transparency Materials	**Inadequate or no Transparency** Patients are not informed about how their personal data is being used through inadequate or lack of transparency material The risk to data subjects is that their personal data is processed in an unfair or unexpected way, potentially causing distress. This would breach the fairness principle 1 of GDPR and Articles 13 and 14. It could also result in data subjects not being aware of their data subject rights.	Reasonable possibility	Some impact	3	Treat	NHS England will make available a template GP Practice Privacy Notice and has published its own Transparency Notice Each research organisation is responsible for obtaining Explicit Consent from each participant (or consent alternatives where the participant is a child or lacking capacity). This process requires participants (or parent/guardian/consultee) to be fully informed of the research study and details of how personal data will be processed. Participants (or parent/guardian/consultee) will be provided with information sheets and consent forms which detail what data the research organisation will collect about the individual. Research organisations are also to be required to notify their participants that they will be obtaining GP data from NHSE before data is shared with them	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-004	Data Provision Notice GP System Supplier GPES	**More data than is necessary for purposes specified in the COVID-19 Public Health Directions 2020 and GPES Data for Consented Research Directions 2026 are shared by GP Practices and Processed by NHS England.** Either because the data items were not all required or because the system for collection takes data items outside of the items covered by the DPN including Restricted Data. The risk to data subjects is of distress caused by processing data about them they did not expect would be shared with or by NHS England.	More than likely	Some impact	4	Treat	Data is already extracted using GPES to meet the requirements of the COVID19 Public Health Directions 2020 which will not pull all coded data but only the codes specified in the extract specification. Under the extraction arrangements carried out by the GP IT System Suppliers, the extractions are therefore limited to data fields that are detailed in the data specifications/business rules. The extract has been in place and data collected under this mechanism since May 2020 without any issues arising. The specifications/business rules around the original GDPPR collection were developed in consultation with potential users of data, including researchers to establish what data is necessary for their use cases and why. There has been further consultation with potential Approved Research Studies regarding the data specification and its utility for non-COVID19 research and it is considered to have significant utility, which is why the GPES Consented Cohort Directions 2026 are being put in place to require this to happen. Legally Restricted Codes will be upheld (e.g. gender recognition) and excluded from the collection. Business rules have been written without the legally restricted codes and limited to SNOMED code sets	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-005	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-006	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-007	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**	**REDACTED**

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-008	Data Access Request Service (DARS) - Data Dissemination	**Breach of security by NHS England in the dissemination of the Collected Data through making the incorrect data available through a DARS data file resulting in the unauthorised disclosure of personal data to third parties and a personal data breach.** The risk to data subjects is distress, anxiety and other harm to the rights and interests	Reasonable possibility	Some impact	3	Treat	The DARS Data Sharing Agreement articulates specification to be provided to the customer. Data production have an assured processes for inputting DSA information to create a data view or extract conforming to the agreement. The extract method has been tested by the assurance team proving that given the correct inputs the correct customer outputs are produced. There is a sign-off process for individual customer extracts whereby a senior manager compared the data produced with the specification in the DSA to ensure these are aligned. There is a controlled process for removing data from an extract should any data breach be identified. A process is in place for reporting any data breaches through the appropriate channels via National Service Desk.	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-009	Data Access Request Service (DARS) - Data Dissemination	**Risk of unauthorised access of the Collected Data within NHS England resulting in the data being used for unauthorised purposes.** The risk to data subjects is that their personal data including special category data is processed by unauthorised third party resulting in distress, anxiety and other harm to the rights and interests of the data subject	Reasonable possibility	Some impact	3	Treat	Access by analysts to the data is governed by the Clear Data Access process and will only be granted by the Information Asset Owner to analysts who extracting data for an Approved Research Study pursuant to an approved DARS DSA following a request by DARS.	Remote	Some impact	2	None	N/A

GP-DPIA-010	Data Access Request Service (DARS) - Data Dissemination	**Risk of data being disseminated to organisations that do not meet the required security standard expected by NHS England.** The risk to data subjects is that their personal data including special category data is subject to a security breach by an Approved Research Study and disclosed to an unauthorised third party resulting in distress, anxiety and other harm to the rights and interests of the data subject.	Reasonable possibility	Serious harm	4	Treat	All Approved Research Studies receiving patient data must meet current NHS security standards for holding patient data. This includes maintaining the required standards under the annual Data Security and Protection Toolkit. Studies will need to demonstrate through the DARS process that they have adequate security measures in place to protect the data where it is to be disseminated to them. Such security requirements are set out as part of the DARS application process and are documented on-line within the DARS section of the NHS England website. There are also specific security requirements that need to be met to satisfy the access criteria under the GP Data for Consented Cohorts Requirements Specification Part of the DARS application process includes checking that the organisations that control/process the data have appropriate safeguards in place for secure handling of the data and they meet the obligations in their data sharing contract and Data Sharing Agreement. If patient data is to be made available to other organisations under a sub-licence from NHS England (**Sub-Licensees**), then all access by Sub-Licensees and their users must be through a Secure Data Environment (**SDE**) that complies with Department of Health and Social Care policy on Secure Data Environments for health and social care data and SDE accreditation requirements. NHS England's cyber security team will assured responses provided by Approved Research Studies regarding how they have met the SDE accreditation requirements. If study SDEs do not meet DHSC policy requirements then a clear plan to achieve this must be in place and they may not make the data available to other organisations until requirements are confirmed as met. Under the terms of the Data Sharing Agreement and the Data Sharing Framework Contract NHS England can also carry out audits on compliance with the Access Criteria, including security requirements. DPST returns will also be monitored annually by NHS England.	Remote	Serious harm	3	Once the NHS SDE accreditation scheme is available research studies must obtain and maintain accreditation on an ongoing basis. Approved Research Studies must obtain accreditation within one year of the accreditation scheme being made available and also	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
											maintain accreditation on an ongoing basis.	
GP-DPIA-011	Direction Transparency Materials	**The Collected Data are used for a purpose outside of what is defined in the General Practice Data for Consented Research Directions 2026 by data recipients.** The risk to data subjects is that their data could be processed for purposes beyond those which they expected and which were set out in the Transparency Notices provided by NHS England and GPs. This could cause the data subject to suffer distress and otherwise impact on their rights and interests including that their data is used for purposes that they might reasonably consider inappropriate or unethical.	Reasonable possibility	Some impact	3	Treat	The DARS application process assesses how the Collected Data is used and an application will only be accepted for approved research purposes where the research study meets the Access Criteria including the criteria set out in the Requirements Specification and the relevant assurance processes have been undertaken. The DARS Data Sharing Agreement for the dissemination of the Collected Data will set out the purposes for which the data can be used and that the data cannot be used for any other purposes, without applying to DARS for a change to the Agreement. DARS publishes details of those with whom it has shared data and the purposes for this in the Data Release Register. NHS England have rights to audit agreement compliance and take action if there are breaches of the agreement. NHS England will proactively audit higher risk data use cases/recipients of data as part of its rolling DARS Data Audit Plan.	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-012	Direction Records Management Data Recipient Consent Process	**The personal data is processed for longer than necessary for the purposes set out in the General Practice Data for Consented Research Directions 2026 by** (i) NHS England (ii) (ii) the data recipient Retaining and processing data for longer than is necessary will cause distress to data recipients.	Reasonable possibility	Some impact	3	Treat	This retention period for the Collected Data is in line with the NHS England Records Management Policy and the NHS Records Management Code. Responsibility for ensuring retention periods are complied with rests with the Information Asset Owner (IAO). IAOs must review all of their Information Assets annually and confirm the Unified Register is up to date as part of the annual NHS England Data Security and Protection Toolkit submission. When data is to be destroyed, it will be destroyed securely with the decision and action recorded in accordance with NHS England's Records and Document Management Policy and Corporate Retention and Disposal Framework: Implementation Process. For data stored on DPS the process for destruction is to carry out a delete action on the relevant data, this takes 180 days for complete destruction as per AWS terms and conditions. Data recipients must specify their intended data processing and retention period in their DARS application, which will relate to the purposes for which they are to process the data. The retention period is specified in the Data Sharing Agreement and a DSA will remain in place for the duration that the data is retained. The DSA will require secure destruction at the end of the permitted period and provision of a signed data destruction certificate from the DPO of the data recipient as evidence the data has been securely destroyed. The appropriateness of the retention period is assessed as part of the DARS process.	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-013	GP System Supplier GPES	**Risk that inaccurate data is collected, analysed and disseminated to authorised organisations** Data will be collected as an initial bulk extract and then on a monthly basis. Due to the monthly extraction frequency, there is a risk that the data may not be up to date at the time of dissemination This could lead to inaccurate data being used for authorised purposes. As the data is being used for secondary use purposes it is unlikely that this will have an impact on the individual concerned.	Remote	Some impact	2	Tolerate	Responsibility for data accuracy within patient records lies with the GP Practices as the source data controller. Where updates are made to GP records, these updates will be collected by NHS England as part of the next data collection. The data collected by NHS England is therefore updated every month. NHS England shall ensure the last date of the collection is clearly known by the recipients of the data to prevent misinterpretation of the data recency. Data extraction frequency will be reviewed and may be increased when there is clear requirement and capacity is available to execute increased frequency.	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-014	Data Access Request Service (DARS) - Data Dissemination Data Recipient Consent Process	**Risk that Collected Data is transferred outside of the UK to a jurisdiction which does not provide for sufficient protections of the rights of data subjects as required under GDPR** The risk to data subjects is that the data protection arrangements in the jurisdiction where processed are not as robust as in the UK and do not provide the same level of safeguards over their data or afford them the ability to exercise their data subject rights in the same way.	Reasonable possibility	Some impact	3	Treat	The geographical location of the data processed by NHS England remains within the UK jurisdiction in the DPS Platform which is hosted in the AWS cloud within the UK. Data recipients must specify the Territory of Use for processing and storage of data in their DARS application. DARS will assess the adequacy of the territories as part of the application process, and the DPO will carry out further assurance, including on certain Transfer Risk Assessments (TRA) and associated processes where data is made available to a country without an adequacy decision. DPO will carry out assurance, with support from internal and external legal support on TRAs and TRA processes if required. The Direction requires Approved Research Studies to be transparent about overseas access and publish countries form which access is granted to ensure that their participants understand this.	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-015	Type 1 Objections Policy	**Type 1 Objections are applied overriding participant consent** The consequences of excluding records with Type 1 Objections from the GPDPPR collection and overriding consent would cause data subjects distress. The risk to data subjects is that the Explicit Consent given to the research organisation for it to obtain GP data via NHS England does not override an existing Type 1 objection.	Reasonable possibility	Some impact	3	Treat	Type 1 objections have been upheld in collecting this data from General Practices under the COVID-19 Directions and therefore the data for those patients who have registered a Type 1 objection with their GP is not contained within the GPDPPR dataset. It is not technically possible currently to include those records of patients who have consented but registered a Type 1 Opt Out, within the dataset. Without this Direction being in place, data about patients who have consented and who haven't registered a Type 1 objection is not being shared by GP Practices in accordance with the wishes of the patient. This solution therefore addresses this issue, but it is recognised that currently the solution does not include these patient's records. This is made clear in Transparency Notices, in DPNs and has been made clear to stakeholders including researchers in consultation and this limitation accepted. Before sharing data with an Approved Research Study this will be made clear to the study. Research organisations can also discuss the implications of having a Type 1 opt out with their Patient and Public Engagement Groups and can provide information to their participants to support their participants to make informed decisions. Type 1 Opt Outs can, where a participant choses, be withdrawn through local processes with their GP practice.	Remote	Some impact	2	None	N/A

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
GP-DPIA-016	Breach of data minimisation if COVID-19 Directions revoked or GPDPPR collection is no longer required under those Directions	These Directions specify NHS England are to collect the GPDPPR dataset and are therefore not dependent on the COVID-19 Directions continuing. If the COVID19 Directions are revoked or the collection no longer required for COVID-19 purposes, NHS England would still be legally obliged to continue to collect the GDPPR data, however the data collection would contain records of patients who have not consented to their data being shared with Approved Researchers as well as those who have consented.				Treat	This risk will be kept under review. At the commencement of the GP Data for Consented Research Service, the data being used is already collected and held by NHSE for COVID-19 purposes. This risk only arises if there is no longer a need for the data to be collected for COVID-19 purposes. Currently there is no other technical solution capable of collecting only consented data for Approved Research Studies which is not cost and resource prohibitive. Therefore this collection is currently the only mechanism for meeting the need of sharing GP data with those large studies who have patient consent. Although ore data may be collected than is strictly necessary, only consented records would be accessed and shared with Approved Researchers in line with the GPES Data for Consented Research Directions 2026 and the data is securely protected				To be reviewed if the COVID-19 collection is no longer required or the COVID-19 Directions are revoked	

GP-DPIA-017	Risk that data is shared for a patient who is not a participant due to a mismatch with NHS number shared with NHSE by the approved research study with their participant	There is a risk that there is an error or a confusion that results in an NHS number being shared with NHSE that does not relate to a patient who has consented.				Treat	DARS has a robust and well established matching process in place that would not return a result if there was not a clear match. A paper on the matching process was shared with CRAG on 1.7.25 who accepted the process.				NHS England will explore adding functionality to the NHS App to show those patients who have consented which research studies are receiving their health data from NHS England, with links to those studies for further information (including routes to ask the research study	Prioritisation against other App demands in early 2026

Risk	Which elements of the initiative give rise to privacy risks?	What is/are the potential or actual privacy risk(s)	Likelihood	Impact	RAG status	Decision on Risk: Tolerate/Terminate/Treat/Transfer	Proposed solution(s)/mitigating action(s) – *systems and processes that are or will be in place and operating that mitigate this risk, including assurances*	Likelihood	Impact	RAG status	Action	Target Date for completion
											for more information or to withdraw their consent)	
GP-DPIA-018	Risk of security breach by Approved Research Studies associated with data being accessed by third party researchers from their SDE	There is a risk that third party access to data held by Approved Research Studies in their SDEs occurs which results in data being shared outside of SDEs in breach of the terms of the DSA with NHS England and/or in breach of UKGDPR				Treat	NHSE Cyber teams will carry out assurance on the security of Approved Research Studies' SDEs and may request that research studies seeking access to this data through the Service carry out and provide additional security assurance as may be assessed necessary by the NHSE Cyber Team. Research studies will not be approved to receive data until they have met all of the Access Criteria, including the security requirements set out in the Requirements Specification.				NHSE to review security access criteria requirements if advice from NHSE or DHSC Cyber teams changes	N/A

19. Further Actions

- The completed DPIA should be submitted to the PTT Helpline Service (**REDACTED**) for review
- The IAO (Information Asset Owner) should keep the DPIA under review and ensure that it is updated if there are any changes (to the nature of the processing and/or system changes)
- A redacted version of the DPIA should be made available to the public

20. Signatories

The DPIA accurately reflects the processing and the residual risks have been approved by the Information Asset Owner:

Information Asset Owner (IAO) Signature and Date

Michael Chapman, 6 Feb 2026

FOR PRIVACY, TRANSPARENCY AND ETHICS AND OFFICE OF THE DPO USE ONLY

21. Summary of high residual risks

Risk no.	High residual risk summary

Summary of DPO advice:

Data Protection Officer (DPO) **Signature and Date**

ICO consultation outcome:

Office of DPO	Signature and Date

Next Steps:

- **DPO to inform stakeholders of ICO consultation outcome**
- **IAO along with DPO and SIRO to build action plan**

Appendix A - Glossary of Terms / List of Abbreviations

Term / Abbreviation	What it stands for/means
AGD	Advisory Group for Data
Approved Research Studies	Specific research studies approved to access GP data under the GPES Data for Consented Research Directions 2026
AWS	Amazon Web Services (https://aws.amazon.com/what-is-aws/?nc2=h_ql_le)
Bucket	In cloud computing buckets are the basic containers that hold data Everything that is stored in cloud storage must be contained in a bucket and they can be used to organise and control access to data.
Clear Data Access	An internal process to control access to data by NHS England staff. Staff must apply for access via a form which must be approved by line managers and the relevant Information Asset Owner to grant access. Staff will only be granted access to those functions or data required to perform their role and access to identifiable data is only granted where there is a specific need that cannot be met using de-identified data.
Explicit Consent	Explicit Consent given by health research participants for a research organisation to access their confidential health information. This includes where parental consent is given on behalf of a child (unless the principle of Gillick Competence is applied). This term also includes individuals lacking capacity, where consultees have given advice that the individual would wish to take part in the research if they were able to give consent themselves as defined in the Mental Capacity Act 2005.
CRAG	Consent for Research Assurance Group
Data Access Request Service (DARS)	A function of NHS England that offers clinicians, researchers and commissioners the data required to help improve NHS service. Data Access Request Service (DARS) - NHS England Digital
Data Extract	Data that is collected from the GP IT systems by GPES over a specified period of time, limited to data fields that are detailed in the data specification / business rules.
DPS	Data Processing Services – the secure technologies and processes used by NHS England to collect, process and access data, and specifically within this DPIA to the platform and series of processes for receiving and transforming national data collected from care provider and other care related organisations (https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services/improving-our-data-processing-services).
DSA	Data Sharing Agreement

GDPPR	GPES Data for Pandemic Planning and Research (COVID-19) (https://digital.nhs.uk/coronavirus/gpes-data-for-pandemic-planning-and-research)
GP Data	Data collected from General Practitioners in England, via their GP system suppliers
GPES	General Practice Extraction Service
MESH	Message Exchange for Social care and Health - service provided by NHS England and is the main secure large file transfer service used across health and social care organisations for clinical and other data. (https://digital.nhs.uk/services/message-exchange-for-social-care-and-health-mesh)
Personal Data	Any information relating to an identified or identifiable individual.
Processing	Any operation performed in Personal Data.
Release of Data	Dissemination of data upon the approval of a data access request by DARS and signing of a data sharing agreement between the data requestor and NHS England.
SDE	Secure Data Environment
SEFT	Secure Electronic File Transfer

Appendix B – REDACTED

REDACTED