NHS England OpenSAFELY Data Analytics Service-: Template data protection impact assessment (DPIA) for GP Practices

Introduction

A data protection impact assessment (DPIA) will help you to identify and mitigate potential data protection risks to an acceptable level before using or sharing (processing) data that identifies individuals (personal data).

A DPIA will also help you meet a number of data protection legal requirements including:

- Data protection by design - privacy and data protection issues must be considered at the start, or in the design phase, of a new system, product or process, then continuously while it exists.
- Accountability - your organisation is responsible for showing how it complies with data protection laws.
- Transparency - personal data must be used and shared in a transparent way.
- Security - adequate measures need to be in place to protect data. This can range from policies and procedures to technical security measures such as encryption of data.

DPIAs are mandatory when there is a high risk to individuals, such as when using the health and care data of a large number of people. The OpenSAFELY Data Analytics Service does not involve using or sharing data in a new way. GP practices will be controllers for the pseudonymised dataset against which queries will be run. Therefore, GP practices should complete a DPIA to provide greater reassurance locally that information governance issues and risks are being managed appropriately.

A DPIA involves a risk assessment. While NHS England believe that high risks have been addressed for the OpenSAFELY Data Analytics service, if you believe that you have identified a new high-level risk that remains after applying mitigations, then you must consult with the Information Commissioner's Office (ICO) for further advice.

A DPIA is a live document - you must update it if there are any changes to:

- the purpose - why you are proposing to use or share personal data
- the manner - how you will use or share the data
- who is involved - the organisations using and sharing personal data

A template DPIA for GP practices can be found in Annex 1. We encourage GP practices to adopt this template. The template is written so that it is easy to use without needing expertise in data protection, but you should consult your data protection officer (DPO) to ensure they are content with the DPIA. It is the responsibility of the organisation which is deciding on why and how the data is being used and shared (known as the controller), to ensure that the DPIA is completed appropriately.

Annex 1

Data protection impact assessment (DPIA) title:
NHS England OpenSAFELY Data Analytics Service

SECTION 1 – SCREENING QUESTIONS

1. **Do you need to do a DPIA?**

   A Data Protection Impact Assessment (DPIA) is a useful tool to help organisations demonstrate how we comply with data protection law.

   DPIAs are also a legal requirement where the processing of personal data is "likely to result in a high risk to the rights and freedoms of individuals".

   By completing a DPIA you can systematically analyse your processing to demonstrate how you will comply with data protection law and in doing so identify and minimise data protection risks.

   a. **Summary of how data will be used**

   The NHS OpenSAFELY Data Analytics Service Pilot (referred to as the Service) provides a secure analytics service for Approved Users (academics, analysts and data scientists) to access pseudonymised GP and NHS England patient data for Approved Projects, this includes

   1. clinical audit;
   2. service evaluation;
   3. health surveillance;
   4. research;
   5. evaluation of the Service; and
   6. health and social care policy, planning and commissioning purposes and public health purposes, where agreed on a project specific basis by or on behalf of:
      - I. the Department of Health and Social Care,
      - II. NHS England, and
      - III. and a nominated representative of each of the Royal College of General Practitioners and the British Medical Association on behalf of the Joint GP IT Committee

The Service uses OpenSAFELY open-source software tools (OpenSAFELY Platform), a Trusted Research Environment, which was developed by the Bennett Institute in collaboration with the Electronic Health Record (EHR) research group at the London School of Hygiene and Tropical Medicine, NHS England, and the GP System Suppliers (GPSS). The Service uses the OpenSAFELY Platform to run project analysis code on pseudonymised GP, pseudonymised NHS England patient data and specific external data providers' pseudonymised data, which is held within TPP or Optum (formerly EMIS).

The Service is designed to keep patient data confidential and enforce on Approved Users the requirement to write into computer code (for public sharing) exactly what subset of patient data they require for each approved project: users write analysis code away from the patient data and test it on dummy data. The Service then automates the running of code (the Queries) across the full coded pseudonymised GP data and linked patient data to generate intermediate pseudonymised datasets specifically tailored to the needs of the project; these study (or project) datasets (Intermediate Outputs) have substantially less detailed information than the full coded pseudonymised GP data as they are a subset of the complete pseudonymised GP and NHS England patient dataset made available by the GPSS . Further queries are run to generate aggregated outputs (the Aggregated Outputs) and logs to help identify and fix errors in the analysis code.

Approved Users can only access the Aggregated Outputs generated by their Query, and review error logs (to help identify and fix errors in their analysis code) inside the GPSS's secure environment. Logs may sometimes contain small amounts of highly refined and pseudonymised data about a small and arbitrarily selected subset of the population to assist researchers with their study code review. A combination of technical and process controls manages the risk of log files disclosing confidential information, which in most circumstances will make the data anonymous in the hands of the Approved User within the platform.

Before any Aggregated Outputs are released outside the GPSS's environment, for wider sharing or publication, Approved Users apply statistical disclosure controls, and the outputs are reviewed and cleared by trained output-checkers; such outputs are considered anonymous. If an Approved User accesses logs that contain data that could be considered a breach of confidentiality, this must be reported through established channels identified via OpenSAFELY - https://docs.opensafely.org/outputs/viewing-released-files/#reporting-a-data-breach, and NHS England - https://digital.nhs.uk/services/data-services-for-commissioners/incident-and-service-request-process.

All actions by all users in the Service are logged in public, in real-time and all Queries are logged and published (). No record level GP or NHS England data leaves the GP system suppliers' environment.

b. Description of the data

[x]	Pseudonymised data - identifiers, for example name or NHS number, are replaced with a unique number or code (a pseudonym)
[x]	Anonymous data - not identifiable, for example trends or statistics

Record-level data, pseudonymised at source, is processed by the Service to deliver intermediate and aggregate outputs containing structured and coded data only

Approved users only have access to view the aggregated outputs generated by their query.

Pseudonymisation and outputs process:

The Service has been built with a focus on patient privacy and protections and, as such aims to mitigate risk using its tools and design.

“Pseudonymisation” is a widely used process for protecting patients’ privacy whereby explicit identifiers such as names, addresses, and dates of birth are removed from patients’ medical records before they are used or shared. Pseudonymisation creates an artificial code for each patient (a pseudonym), which allows that patient record to be linked to other records for the same patient, but without easily identifying who the individual is.

The pseudonymised data is treated as Personal Data, as it is technically possible to re-identify patients from pseudonymised data; but the OpenSAFELY platform and processes use other technical controls and measures to make this very unlikely. In addition, the GP data is not only pseudonymised for direct identifiers and but also further de-identified with respect to most indirect identifiers, ensuring minimal risk of re-identification while maintaining the possibility of secure linkage via pseudonyms. We have described this process as **pseudonymisation and further de-identification**.

Specifically for the GP Data, the following direct and indirect identifiers are removed by the GPSS in the secure GPSS environments:

- Removal of associational identifiers: Mobile phone numbers, email addresses, telephone numbers, hardware and software unique identifiers, IP addresses.
- Removal of transactional unique identifiers: all unique booking reference numbers for appointments, contacts, and referrals.
- Removal of functional unique identifiers: Titles, forenames, middle names, surnames, full dates of birth, full dates of death, house name, house number, street, full postcode.
- Removal of narrative text (commonly referred to as ‘free text’ data: All free text on patient records is removed. In line with other UK primary care research database permissions, the dosage and quantity fields on prescribed medication are retained, but any script notes are removed.
- Removal of additional unstructured context: scanned images, medical drawings, letters, and all other record attachments.
- Derived data items and removal of exact original values: date of birth (MM/CCYY), partial postcodes at sector level, indices of multiple deprivation, the rurality-urban classification, geographic super-output area codes at each super output area level. Note – for organisations, the only geographic indicators stored are the lower super output areas and / or middle-level super output area code and the Local Authority code and STP/ICS code.
- Pseudonymisation is applied to the remaining data: Generation of strong pseudonyms using industry-standard cryptographic hash techniques with only

NHS England approved holders of the keys to prevent re-identification of patients.

The pseudonymised datasets held within the GPSS's systems are then analysed using the OpenSAFELY platform.

The platform allows approved users to design their query and run their code against randomly generated dummy data, before running the actual query as an automated request on the pseudonymised data within the service. This eradicates the need for users to develop their analyses by interacting directly with real pseudonymised patient data and thus eradicates a key historic source of risk for projects where data is accessed at very large population scales.

The datasets (both GP-Controlled and NHSE-Controlled) are queried by the Service. Intermediate Outputs (under NHSE Control) are the results of the Queries. These Intermediate Outputs are then subject to statistical analysis - again *without the users having sight of this data* - to generate Aggregated Outputs.

A limited number of Approved Users can access the Aggregated Outputs within the Service (subject to a Data Access Agreement). The Aggregated Outputs, however, cannot be released/removed from the system or linked with other data. Prior to release from the system, there is a disclosure control process carried out to ensure the Aggregated Outputs cannot identify any individual before they are released from the system for wider sharing or publication. The disclosure control process involves the Approved Users applying disclosure controls to the results they seek to release; these results are then reviewed and cleared for release by trained output-checkers. Such outputs are now considered anonymous. In addition, information relating to specific GP practices and Primary Care Networks (PCNs) is pseudonymised in the data made available to the Service; following agreement with the GP profession, information that could identify individual GP practices or PCNs can only be released as an aggregate output in line with a process agreed between NHS England and a representative of the Joint GP IT Committee.

As per the below diagram in Section 4 question 1, the pseudonymised GP data remains under the control of GP practices (Level 1). The Service automates the running of code (the Queries) against pseudonymised GP data (level 1) and pseudonymised NHS England data (level 2), to generate intermediate pseudonymised datasets (Intermediate Outputs) in Level 3, and then final aggregated outputs (the Aggregated Outputs) in Level 4.

SECTION 2 - WHY DO YOU NEED THE DATA?

1. **What are the purposes for using the data?**

The purpose is to provides a secure analytics service for **Approved Users** (academics, analysts and data scientists) to access pseudonymised GP and other linked patient data for

- clinical audit[1];
- service evaluation[2];
- health surveillance[3];
- research[4];
- evaluation of the Service; and
- health and social care policy, planning and commissioning purposes and public health purposes, where agreed on a project specific basis by or on behalf of:
  - the Department of Health and Social Care,
  - NHS England, and
  - a nominated representative of each of the Royal College of General Practitioners and the British Medical Association on behalf of the Joint GP IT Committee

NHS England and Approved Users need insights from this vital data to analyse and link data for research, clinical service evaluation, clinical audit and health surveillance which will help improve the quality of people's lives and help save lives.

The purposes for which this data may be analysed and used include:

- understanding risks to health, trends in diseases and such risks, and controlling and preventing the spread of diseases and such risks
- identifying and understanding information about patients or potential patients with, or at risk of disease
- understanding information about patient access to health services as a direct or indirect result of illness, and the availability and capacity of those services
- health services research on changes in clinical activity and population health and impact, as well as consequences of this
- informing the development

2. **What are the benefits of using the data?**
   NHS England and Approved Users need insight from this vital data to analyse and link data for research, clinical service evaluation, clinical audit and health surveillance which will help save lives.

   Supporting such research via the Service will reduce the burden on General Practice, the wider NHS (including hospital, community and mental health services), as well as provide increasing support to social care services; all at a time when demand on resources is high. It is hoped the insights will support General Practice and the wider health and care system to improve the quality and safety of care and support to patients better.

[1] As defined in the https://www.hra-decisiontools.org.uk/research/docs/DefiningResearchTable_Oct2022.pdf

[2] As defined in the https://www.hra-decisiontools.org.uk/research/docs/DefiningResearchTable_Oct2022.pdf

[3] As defined in the https://www.hra-decisiontools.org.uk/research/docs/DefiningResearchTable_Oct2022.pdf

[4] As defined in paragraph 3.1 pf the UK Policy Framework for Health and Social Care Research - Health Research Authority

SECTION 3 - WHAT DATA DO YOU WANT TO USE OR SHARE?

1. Can you use anonymous data for your purposes? If not, explain why.

[X]	No The GP data will be matched to NHS England controlled datasets; this is done via the use of a common pseudonymisation process. Matching would not be possible if the data was anonymous. However, any data that is shared because of the analysis is aggregated and disclosure controlled.

2. Which types of personal data do you need to use and why?

Data Categories [*Information relating to the individual's*]	**YES/ NO**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]* ***FOR CLARITY: NOT ALL DATA ITEMS ARE USED IN EVERY CASE FOR EVERY APPROVED PROJECT.*** ***Any of the data items that are supported to be accessed via the OpenSAFELY technology are subject to robust governance controls, including the Project approval process, that will only allow the processing of specific data items, where it is necessary for the project***
Personal Data		
Name	NO	
Address	NO	
Postcode	YES	Agreed as part of project governance controls, on a project by project basis, as required **partial** postcodes are processed. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease. E.g. areas of geographical depravation.
DOB	YES	Agreed as part of project governance controls, on a project by project basis, as required Partial DOB in format MM-YYYY. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease. This variable informs calculation of age
Age	YES	Agreed as part of project governance controls, on a project by project basis, as required. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease.
Sex	YES	Agreed as part of project governance controls, on a project by project basis, as required. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention disease.

Commented [JG1]: Why is postcode needed for these purposes? This doesn't explain

Data Categories [*Information relating to the individual's*]	**YES/ NO**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]* ***FOR CLARITY: NOT ALL DATA ITEMS ARE USED IN EVERY CASE FOR EVERY APPROVED PROJECT.*** ***Any of the data items that are supported to be accessed via the OpenSAFELY technology are subject to robust governance controls, including the Project approval process, that will only allow the processing of specific data items, where it is necessary for the project***
Marital Status	YES	Agreed as part of project governance controls, on a project by project basis, as required It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease. Through the identification and processing of the data item necessary for approved projects subject to robust governance arrangements being implemented. Many ethical and valid studies exist in journals that have processed marital status, so the use of such a code is not contentious nor novel; and like many studies, researchers will discuss in their papers the limitations and strengths of their studies, which where necessary will include aspects related to marital status.
Gender	YES	Agreed as part of project governance controls, on a project by project basis, as required. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease.
Living Habits	YES	Agreed as part of project governance controls, on a project by project basis, as required It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease. E.g. smoking, alcohol consumption, exercise habits
Professional Training / Awards / Education	NO	
Income / Financial / Tax situation / Financial affairs	NO	
Email Address	NO	
Physical Description	YES	Agreed as part of project governance controls, on a project by project basis, as required. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease.
General Identifier e.g., NHS No	YES	Agreed as part of project governance controls, on a project by project basis, as required. NHS Numbers are pseudonymised to protect the identity of patients it is used to link datasets within the secure data environment.
Home Phone Number	NO	
Online Identifier e.g., IP Address/Event Logs	NO	
Website Cookies	NO	

Data Categories [*Information relating to the individual's*]	**YES/ NO**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]* ***FOR CLARITY: NOT ALL DATA ITEMS ARE USED IN EVERY CASE FOR EVERY APPROVED PROJECT.*** ***Any of the data items that are supported to be accessed via the OpenSAFELY technology are subject to robust governance controls, including the Project approval process, that will only allow the processing of specific data items, where it is necessary for the project***
Mobile Phone / Device No / IMEI No	NO	
Location Data (Travel / GPS / GSM Data)	NO	
Device MAC Address (Wireless Network Interface)	NO	
Banking information e.g., account number, sort code, card information	NO	
Special Category Data		
Physical / Mental Health or Condition	YES	It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease.
Sexual Life / Orientation	Partial	Agreed as part of project governance controls, on a project by project basis, as required. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease. Data is collected and processed except: a. SNOMED Refset for 'General Practice summary data sharing exclusion for gender related issues' 999004371000000109 b. SNOMED Refset for 'General Practice summary data sharing exclusion for assisted fertility' 999004351000000100 c. SNOMED Refset for 'General Practice summary data sharing exclusion for termination of pregnancy' 999004361000000107 d. All children of the SNOMED code 118199002 'Finding related to sexuality and sexual activity'
Religion or Other Beliefs	YES	Agreed as part of project governance controls, on a project by project basis, as required. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease.
Trade Union membership	NO	
Racial / Ethnic Origin	YES	Agreed as part of project governance controls, on a project by project basis, as required. It is necessary to identify risk factors, treatment options that might improve outcomes and approaches to treatment, and prevention of disease.
Biometric Data (Fingerprints / Facial Recognition)	NO	

Data Categories [*Information relating to the individual's*]	**YES/ NO**	**Justify** *[there must be justification for processing the data items. Consider which items you could remove, without compromising the purpose for processing]* ***FOR CLARITY: NOT ALL DATA ITEMS ARE USED IN EVERY CASE FOR EVERY APPROVED PROJECT.*** ***Any of the data items that are supported to be accessed via the OpenSAFELY technology are subject to robust governance controls, including the Project approval process, that will only allow the processing of specific data items, where it is necessary for the project***
Genetic Data	NO	We believe the answer is "no": we may have access to genetic diagnostic codes, for example stating that someone has a disease with a genetic component (e.g., "Down's Syndrome") but we do not have access to individuals' complex genome or actual gene sequencing information as these are not typically stored as structured or coded data in GP records.
Criminal convictions / alleged offences / outcomes / proceedings / sentences	YES	Agreed as part of project governance controls, on a project by project basis, as required, As SNOMED codes, not free text, where a GP has (infrequently) chosen to capture such coded information relating to this as part of the health record.

Additional datasets that are controlled by NHS England and approved to flow into the GP System Suppliers TPP and EMIS is as follows:

- SUS data (APCS, ECDS, OPA)
- Patient data from ONS Death records (since Feb 2020)

3. Who are the individuals that the data relates to?

[x]	Patients: The patient population made available within the Service for analysis is defined as all patients EXCEPT: - Patients who have registered a Type 1 Opt-Out with their GP Practice - Patients who have no period of registration (in a TPP or EMIS practice) after 1 January 2009 or who died before 1 January 2009 - This means that for each GP System Supplier if there has been any period of registration after 1 January 2009 then all the patient's data from the last practice with that GP System Supplier is available to the Service for analysis, irrespective of the patient's current registration status

4. Where will your data come from?

Data will be collected from all EMIS and TPP GP Practices in England. The GP practices use GP System Suppliers to store the patients' GP record. The record contains only data that GPs have already obtained from patients and other third parties, including other healthcare professionals, for the purposes of providing healthcare services to patients. It is not collected directly from the individuals themselves.

Further data sources will be provided (see further details in Section 3 question 2) and placed in EMIS and TPP alongside the GP data to allow queries to run against both GP and NHS England data sources.

5. Will you be linking any data together?

[X]	Yes The GP data will be matched to NHS England controlled datasets. The NHS England controlled datasets and GP data can be matched through the common pseudonymisation process; it should be noted that any Type 1 Opt-outs are maintained within the GP dataset.

Explanation of the linking process:
There are two methods used for matching the pseudonym.

1. Matching by external data provider: EMIS or TPP sends a file of all their patient pseudonyms to the external data providers; only patient records with a match in the external databases are transferred back into the Level 2 environments in Optum (formerly EMIS) and TPP. This is the preferred mechanism as it minimises unnecessary data flow.
2. Matching by the GPSS : On some occasions (due to technical constraints of the external database provider or when the external provider's population is much smaller, relative to that of the GP population), the pseudonym matching occurs inside the Level 2 environment in Optum (formerly EMIS) and TPP. This involves a two-step process:
    a. The external data provider makes available one file of their full pseudonym list to the GPSS which in turn establish a list of matches of the pseudonyms they have. Each GPSS sends back a list of these matched pseudonyms to the external data provider in a file.
    b. The external data provider then prepares separate files for each of the data sets according to the matched list they were provided with. The two separate files produced by the external data provider, one for Optum (formerly EMIS) and one for TPP, contain the additional requested and approved data for only the matched pseudonyms. This data is then made available to be added to the Level 2 environment in EMIS and TPP.

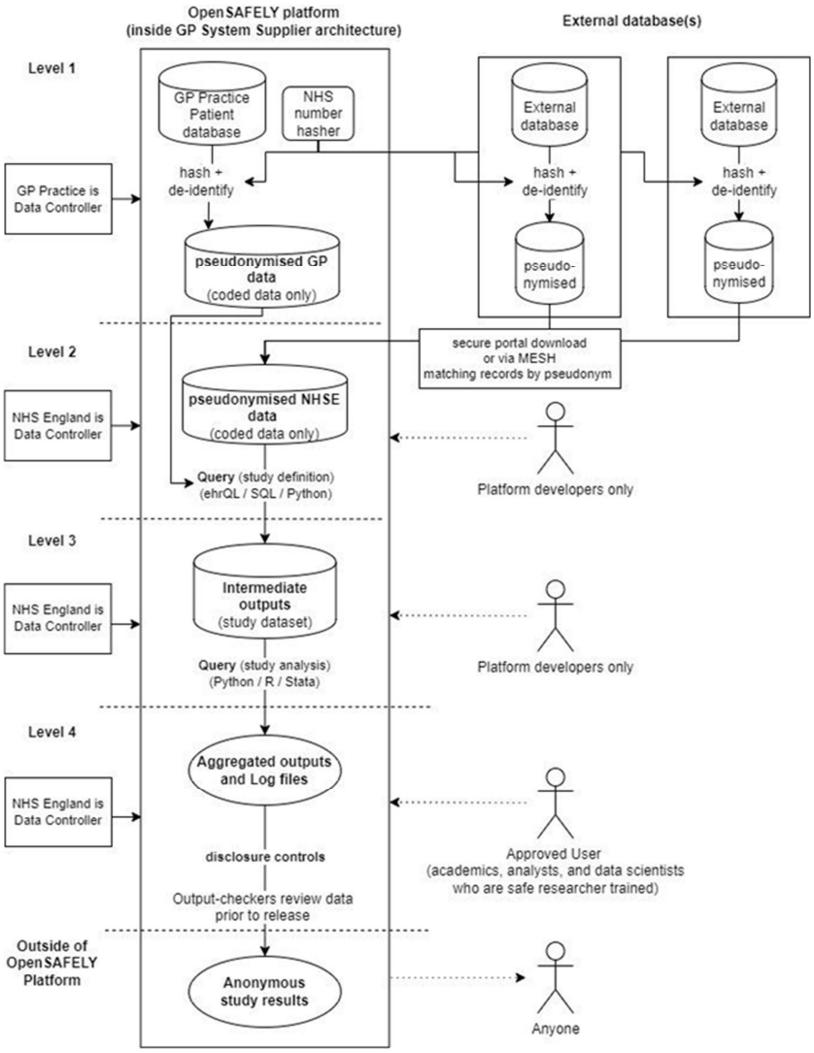
For record linkage, the pseudonyms will be produced by the GPSS who will hold the keys. This pseudonym (with additional data items used where necessary) provides significant confidence in matching accuracy, ensuring that the right record is linked to the right primary care record. Research models will be automatically executed as required for analysis. GP patient data held by the GPSS is incrementally updated to reflect changes made by clinicians in England GP practices.

a. Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?

[X]	Unlikely – see risk table

SECTION 4 - WHERE WILL DATA FLOW?

1. Describe the flows of data.



2. **Confirm that your organisation's information asset register (IAR), record of processing activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.**

[X}	Yes
[ ]	No
[ ]	Unsure

3. **Will data be shared outside of the UK?**

[x]	No The geographical location of the data once transferred to the GPSS is within the UK jurisdiction in their secure environments, which are hosted in the AWS cloud within the UK. All NHS England staff and contractors accessing the data store will be doing so from within the UK. The OpenSAFELY software platform was built by the Bennett Institute and operates from the UK. The NHS England Data Sharing Agreements (for the OpenSAFELY data) restricts the use to defined territories. The application process includes assessing the recipient's legal basis for processing data within these territories. This is reviewed and approved by NHS England according to the UK GDPR and the NHS England Records Management Policy.

SECTION 5 - IS THE INTENDED USE OF THE DATA LAWFUL?

1. **Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?**

[x]	(c) **We have a legal obligation** - the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.

2. **If you have indicated in question 6 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?**

[x]	(g) **We need to comply with our legal obligations to provide information where there is a substantial public interest** Legal obligation by virtue of the above Directions

	UK GDPR – Article 6 basis: UK GDPR Article 6(1)(c) - processing is necessary for compliance with a legal obligation to which the controller is subject (the Directions). UK GDPR Article 9 basis: UK GDPR Article 9(2)(g) - processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject, by virtue of compliance with a direction supplemented by: Data Protection Act 2018 basis Data Protection Act 2018 (DPA 2018) Schedule 1, Part 2, paragraph 6: Statutory etc and government purposes.
[X]	(h) **We need it to comply with our legal obligations to provide or manage health or social care services**

Commented [LW2]: @TREDDENICK, Joanne (NHS ENGLAND) could you check this please?

Commented [JT3R2]: done

3. What is your legal basis for using this health and care data under the common law duty of confidentiality?

[x]	Legal requirement

a. Please provide further information or evidence.

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 ('the Act') 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 Act. This includes where it has been directed to establish an information system by the Secretary of State for Health and Social Care.

The data, as specified by NHS England in the associated Data Provision Notice (DPN), is required to carry out its functions conferred on it by The NHS OpenSAFELY Data Analytics Service Pilot Directions 2025, through the

OpenSAFELY technology. Therefore, organisations that are in the scope of the notice are legally required, under section 259(5) of the Act, to provide the data in accordance with the DPN.

SECTION 6 - HOW ARE YOU KEEPING THE DATA SECURE?

1. **Are you collecting information?**

[x]	No

2. **Are you storing information?**

[x]	Yes

The pseudonymised at source dataset is generated as a result of this service and stored in the secure TPP and Optum (formerly EMIS) GP System Supplier environment. (see Annex 4)

   a. **How will information be stored?**

[x]	Local organisation servers – The NHS owned data stores in TPP are held on servers using Microsoft Server software.
[x]	Cloud storage – The NHS owned data stores in Optum are based on AWS Cloud data centres.

3. **Are you transferring information?**

[x]	Yes

   a. **How will information be transferred?**

   Relevant data from external controlled sources are transferred into each of the secure GP System Supplier environments through a secure portal download or through the MESH.

4. **How will you ensure that information is safe and secure?**

[x]	Encryption	
[x]	Password protection	all users have a password to access the service
[x]	Role based access controls (RBAC)	where users only have access to the data held digitally which is needed for their role (this includes setting folder permissions)
[x]	Business continuity plans	

[x]	Security policies	
[x]	Other	The data stores in Optum (formerly EMIS) is based on AWS Cloud data centres, which are certified for compliance with ISO/IEC 27001:2013 (IT - security techniques - information security management systems), 27017:2015 (IT - security techniques – code of practice for information security controls based on ISO/IEC 27002 for cloud services), 27018:2019 (IT - security techniques - code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors) and ISO/IEC 9001:2015 (quality management systems). Certification details are available at https://aws.amazon.com/compliance/iso-certified/. AWS also possess a 'Standards Exceeded' Data Security and Protection Toolkit (DSPT) which has been reviewed and approved by the NHS England DSPT Team. (quality management systems). Certification details are available at https://aws.amazon.com/compliance/iso-certified/. AWS also possess a 'Standards Exceeded' Data Security and Protection Toolkit (DSPT) which has been reviewed and approved by the NHS England DSPT Team. Data in transit will be protected by standard security policies available for AWS Elastic load balancers and application load balancers (https://docs.aws.amazon.com/elasticloadbalancing/latest/network/create-tls-listener.html) For the TPP data store the TPP infrastructure involves a Tier 3 data centre accredited to NHS England standards for centrally hosted clinical systems and a secure office environment. TPP is accredited to the ISO 27001 standard and is IG Toolkit version 2 compliant. The same governance, security and audit protocols that apply to the production TPP SystmOne environment will extend to cover this data store. This includes the security and audit arrangements required for the NHS GP IT Futures programme (GPITF) and the Health & Justice Information Services programme (HJIS), for example. <u>Pseudonymisation, de-identification and minimisation at source (Process)</u> No free text information or directly identifiable patient information is ever transferred to the Service; redundant data is pruned (for example, the datasets available to the NHS OpenSAFELY Data Analytics Pilot Service do not contain the full data schema for SUS data, but a subset); and data about patient geographic locations is always rounded up to the least disclosive level that is

		still analytically useful (typically, MSOA level for patients, and Integrated Care System level or Local Authority code for organisations). The level of data available is all publicly documented. Identifiable patient information within the GPSS environments (and other data provider organisations) is further de-identified according to the processes outlined in this DPIA (above). In all cases, a pseudonym is created with the patient's NHS number in combination with a salt using the SHA2 512 cryptographic hash technique. The salt is shared by the GPSS with the external data provider: it is emailed as an encrypted file to a specific individual in the external data provider organisation post approval from NHS England. A member of either GPSS then calls the individual and provides the decryption key to unencrypt the salt. There is no directly identifiable data being processed under the scope of this DPIA. It is acknowledged that the sources of the data being provided (e.g., GP Practices) have access to the identifying data, but that is outside of the scope of this DPIA. The OpenSAFELY analytics tool operates a tiered security model, described here: https://docs.opensafely.org/security-levels/. Identifiable data is accessible only in Level 1: this is not available to any Approved users or developers. Level 1 is the data held within the direct care servers of the GPSS, who operate as data processors for GP practices, or the external source data provider environments. In addition, Level 1 is where the pseudonymised and further de-identified GP data is created and stored, which remains under the control of GP practices. The Service automates the running of code (the **Queries**) against pseudonymised GP data (level 1) and pseudonymised NHS England data (level 2), to generate intermediate pseudonymised I datasets (**Intermediate Outputs**) in Level 3, and then final anonymous aggregated outputs (the **Aggregated Outputs**) in Level 4 (See Data Flow Diagram). Pseudonymised and aggregate data is accessed via a secure encrypted connection provided by the **system providers**, within their main warehousing infrastructure. Only aggregated data (after disclosure controls have been applied, as part of the Five Safes Framework) leave the secure environments within EMIS and TPP.

5. How will you ensure the information will not be used for any other purposes beyond those set out in question 2?

[x]	Data processing agreement	
[x]	Data access agreement	
[x]	Audit	
[x]	Staff training	
[x]	Governance and service models	The governance and service model includes: ● Application stage – applications are assessed to ensure that: ● The application is for research, clinical audit, service evaluation and health surveillance purposes. ○ Applications for a health and social care policy, planning and commissioning purposes and public health purposes, where agreed on a project specific basis by or on behalf of: ▪ the Department of Health and Social Care, ▪ NHS England, and ▪ a nominated representative of each of the Royal College of General Practitioners and the British Medical Association on behalf of the Joint GP IT Committee ● The data necessary to support the purpose of the application is available in the system. ● The applicant has submitted a completed application form, along with any relevant supporting documentation ● If the application is for research, that a favourable opinion is provided by an NHS Research Ethics Committee (REC) where required; ● If the application is for clinical audit, service evaluation and health surveillance purposes, that the purpose has had review from a local or institutional ethics committee (to ensure the purpose it is appropriately categorised), or the HRA decision tool is used[5] where there is no local or institutional ethics committee to provide review.

[5] https://www.hra-decisiontools.org.uk/research/

		Further detail surrounding the OpenSAFELY application process can be found here: https://jobs.opensafely.org/apply/
[x]	Technical controls	• Data is pseudonymised and further de-identified at source; linkage of datasets is managed inside by the GPSS systems. The requirement to exclude patients' data for analysis and the Purposes through Type 1 Opt Outs is applied through the OpenSAFELY software. The OpenSAFELY software requires access to a pseudonymised list of patients who have registered a Type 1 Opt-Out. Their opt-out is upheld (i.e. their data is not made available to any Approved Projects) when a Query is run. • No system administrators or platform developers have access to the pseudonymisation key. No event level or patient level data leaves the service (i.e., the secure network boundaries of the GPSS' environments). Users must specify up front the code they are using to analyse the patient data: explicitly writing studies as "analysis code" means that it is possible for any interested party to check exactly how patient data was processed, and to assess if such processing is in line with the approved project purpose; the platform principles also require that all analysis code is made public. It is accepted that some code may remain private while an analysis is in development. However, all code is published when the results of the analysis are shared (or, for non-complete projects, as soon as possible, usually at the point of their cessation, and no later than 12 months after any code has been executed against the raw patient data). System administrators can control when analysis code is made public to maintain our transparency principles. Approved Users can only access their study aggregated outputs and any error logs (if produced) over a secure encrypted connection. Access to the aggregated outputs is via a secure encrypted connection, unique to each user, with all access audited. In addition, all researcher actions in the Service are logged in public, in real-time and all Queries are logged and published (https://jobs.opensafely.org/).

[x]	People controls	● All Approved Users must pass safe researcher training (such as that provided by the ONS or UK Data Service) to have access to the secure environment (Level 4) hosting the aggregated outputs. All Approved users who write study code or access the Level 4 environment, and all output checkers, must sign a Data Access Agreement approved by NHS England. All Approved new users have a 'co-pilot' who is an expert user providing appropriate training and support to ensure safe practice is followed and plausible results are generated.
[x]	Output checking	● Approved Users apply disclosure controls to their study aggregate outputs they request for release from the secure environment. All aggregate outputs are then independently checked to ensure that they are non-disclosive and safe to release by output checkers who have been suitably trained.
[x]	Transparency	● All code run using the system is published online (https://jobs.opensafely.org/), and Approved Users are asked to share links to the papers, reports, blogs and other material (such as presentations) that have been approved for publication on their public facing project page (project pages can be found by following links from these respective organisations,) https://jobs.opensafely.org/organisations/. An example project page showing a link to a paper is found here: https://jobs.opensafely.org/comparative-vaccine-effectiveness/). A list of key papers published in peer-reviewed journals is listed here: https://www.opensafely.org/research. All accepted applications have their study purpose, responsible organisation and study lead information published online.

SECTION 7 - HOW LONG ARE YOU KEEPING THE DATA AND WHAT WILL HAPPEN TO IT AFTER THAT TIME?

1. **How long are you planning to use the data for?**

The Service will be delivered under the NHS OpenSAFELY Data Analytics Service Pilot Directions 2025 until they expire 31st March 2027.

2. **How long do you intend to keep the data?**

   GP practices are the controllers for the GP pseudonymised dataset and will retain the data in line with the NHS Records Management Code of Practice. NHS England is the controller for the data it puts in and for the linked datasets. The retention period for NHS England-controlled data is in line with the NHS England Records Management Policy and the NHS Records Management Code of Practice. The pseudonymised and de-identified patient-level summary data will be retained for at least 2 years for verification of analyses and for audit proposes.

   As the NHS data stores are held with the processors TPP and Optum (formerly EMIS), the data will be held for verification of findings and audit purposes and can be deleted once outside the retention periods, however the data cannot be transferred to other NHS England systems (as per operating requirements set out by the Secretary of State).

3. **What will happen to the data at the end of this period?**

   The following relates to the pseudonymised data generated as a result of the Service. The source data is outside of the scope of this DPIA.

[x]	Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction) – by the processors TPP and EMIS in line with the NHS England Records Management Policy and the NHS Records Management Code of Practice.
[x]	Extension to retention period – with approved justification

   There are no new responsibilities for GP practices regarding the data at the end of the retention period.

SECTION 8 - HOW ARE PEOPLE'S RIGHTS AND CHOICES BEING MET?

1. **How will you comply with the following individual rights (where they apply)?**

Individuals (data subjects) have the following rights under 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 to GP Practices. These will be aligned accordingly to reflect the changes described in the DPIA and DPN. The existing privacy notice on the NHS England website will also be updated. In addition, all research projects using OpenSAFELY software are made public here: https://www.opensafely.org/approved-projects/
The right of access	The Right of access (NHS England) An explanation about how an individual can request a copy of information that NHS England holds is published at: https://digital.nhs.uk/article/6851/How-to-make-a-subject-access-request. Due to the pseudonymisation of the data held within the GPSS environments, it would require a re-identification of the records to provide details of the data used in the Service. Consequently, NHS England will provide information of the source data that NHS England holds on an individual. The right of access (GP Practices) Any patient can make a subject access also request to see part or the whole of their medical records from 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 of access (other sources) - For data originating from non-NHS England sources, patients can make their requests directly with the source providers (as noted on the following website - Data Sources - OpenSAFELY documentation).
The right to rectification	The right for individuals to have inaccurate personal data rectified, or completed if it is incomplete, NHS England via the Service cannot uphold this right, as the Service does not re-identify patients; however, individuals can make a request to either the GP Practice or the source data provider to rectify any errors.
The right to erasure	The right to erasure - the right of erasure does not apply as the legal basis of processing under UKGDPR is not consent or legitimate interest.
The right to restrict processing	Where an individual contests the accuracy of their personal data NHS England will consider the request. An individual can also restrict processing by applying a Type 1 Opt-out through their GP.
The right to data	This is not applicable to this processing because under article 20 (3) the processing is being carried out in the exercise of official

portability	authority vested in the controller under Article 6(1)(c) legal obligation under the NHS OpenSAFELY Analytics Service Pilot Directions 2024 or under Article 6(1)(e) public task.
The right to object	This is not applicable to this processing as the data is being processed under legal obligation.
Rights in relation to automated decision making and profiling	No automated decision making takes place as part of this processing.

2. **Will the national data opt-out need to be applied?**

[x]	No – The National Data Opt-Out allows patients to opt out of their confidential patient information being used for research or planning purposes. If you have registered a National Data Opt-Out, your data will still be processed by NHS OpenSAFELY Data Analytics Service, with certain exceptions[6]. This is because the National Data Opt-Out does not apply where NHS England has a legal obligation to operate the service under the NHS OpenSAFELY Data Analytics Service Pilot Directions 2025. The National Data Opt-Out also does not apply to aggregate anonymous data (data which does not identify you) which is the only data shared with approved users of the OpenSAFELY service.

Type 1 opt outs
Patients that have registered a Type 1 objection with the GP practice will not have their data shared with the Service (or any other organisation outside of their GP practice for purposes other than direct care).

3. **Will any decisions be made in a purely automated way without any human involvement (automated decision making)?**

[x]	No

4. **Detail any stakeholder consultation that has taken place.**

[6] In certain limited circumstances and where project approvals support it, a project may wish to apply the National Data Opt Out (NDOO) as part of the code they have developed, notwithstanding that the Service operates under an exemption to the National Data Opt Out Policy.

Commented [NL4]: Updated the wording in this section to directly align with the NHSE transparency Notice for the service

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 the Direction and this Requirements Specification, the Department of Health and Social Care and NHS England have consulted the following organisations:

- GP Representatives including from:
    - The British Medical Association
    - The Royal College of General Practitioners (RCGP)
- NHS England's Advisory Group for Data (AGD)
- Citizen Juries
- UseMyData
- The National Data Guardian for Health and Social Care
- The Data Alliance Partnership Board (DAPB)
- The Phoenix Partnership Ltd (Leeds) (TPP)
- Egton Medical Information Service Ltd (EMIS)
- NHS England's OpenSAFELY Oversight Board
    - Organisational Members
        - The Bennett Institute
        - Wellcome Trust
        - Open Data Institute
        - London School of Hygiene & Tropical Medicine
        - NHS England
        - RCGP
        - BMA
        - MedConfidential
        - EMIS
        - TPP
        - Association of Professional Healthcare Analysts (AphA CIC)
    -

SECTION 9 - WHICH ORGANISATIONS ARE INVOLVED?

1. **List the organisation(s) that will decide why and how the data is being used and shared (controllers).**

    1. GP Practices are controllers of GP patient data within the clinical systems.
    2. NHS England ingests other (non-GP controlled) pseudonymised data (for which NHSE is the controller) within the secure boundaries of the GP System Suppliers. Details can be found in Section 4 above.

    See Annex 3 for more details on controllers.

2. **List the organisation(s) that are being instructed to use or share the data (processors).**

    The Phoenix Partnership (TPP), and Optum (formerly Egton Medical Information Systems (EMIS))known as the GP System Suppliers are processors for the Service.

3. **List any organisations that have been subcontracted by your processor to handle data.**

    Optum (formerly EMIS) have sub-contracted AWS to support their data stores.

4. **Explain the relationship between the organisations**

    The Service is operated by NHS England (as the data controller) with the Bennett Institute for Applied Data Science (University of Oxford) (as data processor) and The Phoenix Partnership (Leeds) Ltd (TPP), or Optum (formerly Egton Medical Information Systems Ltd (EMIS)) (the GP System Suppliers; also as data processors). The data protection roles are explored further in this document.

    The Service uses OpenSAFELY open-source software tools (OpenSAFELY Platform), a Trusted Research Environment, which was developed by the Bennett Institute in collaboration with NHS England, and the GP System Suppliers (GPSS). The Service uses the OpenSAFELY Platform to run project analysis code on pseudonymised GP, pseudonymised NHS England patient data and specific external data providers' pseudonymised data, which is held within TPP or Optum.

5. **What due diligence measures and checks have been carried out on any processors used?**

[x]	**Data Security and Protection Toolkit (DSPT) compliance**	for the Phoenix Partnership (TPP) – "Standards Exceeded" and Optum Health – "Standards Exceeded"

[x]	**Registered with the Information Commissioner's Office (ICO)**	for the Phoenix Partnership (TPP) registration number Z1927388 and the Optum registration number Z2670786
[x]	**Digital Technology Assessment Criteria (DTAC) assessment**	for the Phoenix Partnership (TPP), and Optum – assessed and approved by NHS England
[x]	**Stated accreditations**	for The Phoenix Partnership (TPP), and Optum (formerly Egton Medical Information Systems (EMIS)) are available on their respective websites or on the NHS Buying Catalogue for Digital Solutions (TPP, EMIS)
[x]	**Cyber Essentials or any other cyber security certification**	for the Phoenix Partnership (TPP), and Optum (formerly Egton Medical Information Systems (EMIS)) are available on the NHS Buying Catalogue for Digital Solutions (TPP, EMIS).

Risk ref no.	**Description**	**Risk score* (L x I)**	**Mitigations**	**Risk score* with mitigations applied**
01	GP practice does not have appropriate transparency materials explaining how the data is used	6	NHS England has provided template wording to GP practices that can be used to update existing privacy notices. Existing privacy notices are likely to reference data sharing in line with legal requirements, which would cover this processing.	4
02	GP practice's record of processing activities (ROPA) is not updated to capture this processing	4	NHS England will remind GPs when disseminating materials for OpenSAFELY that their record of processing activities (ROPA) needs to be updated.	2
03	There is a risk that patient confidence regarding NHS England's use of data is impacted due to a lack of historic or	4	- GPs provided with transparency materials and privacy notices - Transparency and public facing materials	2

	current patient awareness regarding the service and the data it uses, which could lead to negative sentiment and increased opt-outs. There is a particular concern that there is a lack of clarity around controllership by the public which could lead to concern and confusion.		will be further updated to reflect the new service - Further public consultation to be undertaken and future engagement plan to be developed and implemented - NHS England will update its own webpages to provide transparent and timely information about the service and decision making	
04	There is a risk of cybersecurity threats to the service, which could effect the integrity, availability and confidentiality of the personal data held within the service. There is a risk that there are insufficient technical measures in place to ensure the security of the data. There is a risk that the service has not been technically assured as with other services, and that risks could exist that have not been mitigated.	12	The data is held within the data centres of the two core GP System Suppliers (GPSS) TPP and Optum (formerly EMIS). These organisations are subject to all safeguards and controls covered under existing contracts as part of the GPIT Frameworks, which mitigate and manage cybersecurity risks and uphold reasonable technical measures to protect data held within their environments. NHS England may choose to make use of the Audit Clauses within the Data Processing Agreements (DPAs) with the GPSS Service operates to the ONS Five Safes model. Users must be from verified institutions and the projects must have a clear sponsor, this reduces the likelihood of individuals who intend to misuse the data being granted access. Independent cyber specialist have been tasked to carry out end to end review of OpenSAFELY	8

			with a report that will be delivered to OS Programme Board	

***Risk scoring table**

		Impact (I)				
		Negligible (1)	**Low (2)**	**Moderate (3)**	**Significant (4)**	**Catastrophic (5)**
Likelihood (L)	**Rare (1)**	**1**	**2**	**3**	**4**	**5**
	Unlikely (2)	**2**	**4**	**6**	**8**	**10**
	Possible (3)	**3**	**6**	**9**	**12**	**15**
	Likely (4)	**4**	**8**	**12**	**16**	**20**
	Almost certain (5)	**5**	**10**	**15**	**20**	**25**

1. **Detail any actions needed to mitigate any risks, who has approved the action, who owns the action, when it is due and whether it is complete.**

Risk ref no.	Action needed	Action approver	Action owner	Due date	Status e.g. outstanding/ complete
01	Ensure privacy notice updated to capture OpenSAFELY processing	GP practice	GP practice	18/12/25	Complete
02	Ensure record of processing activities has been updated with OpenSAFELY processing	GP practice	GP practice	18/12/25	Complete

SECTION 11 - REVIEW AND SIGN OFF

Reviewer sign-off	
Reviewer name:	**Navaira Mylecent**
Reviewer job title:	**Reception Manager and IG Lead**
Reviewer contact details:	**01273 523 623 sxicb-bh.parkcrescenthc@nhs.net**
Date of review:	**18/12/2025**
Comments:	
Date for next review:	**18/12/26**

Approver sign-off	
Approver name:	**Bret Stevenson**
Approver job title:	**Practice Manager**
Approver contact details:	**bretstevenson@nhs.net**
Date of approval:	**16/01/2026**
Comments:	

Annex 2

The laws that health and care organisations rely on when using your information

Data protection laws mean that organisations must identify which law they are relying on when sharing information. For example if an organisation is sharing information because they are required by law to do so, they need to identify which law is requiring this. The following are the most likely laws that apply when using and sharing information in health and care. This list is not exhaustive.

Abortion Act 1967 and Abortion Regulations 1991
Requires that health and care staff share information with the Chief Medical Officer about abortion treatment they have provided.

Access to Health Records Act 1990
Allows access the health records of deceased people, for example to personal representatives or those who have a claim following the deceased person's death.

Care Act 2014
Defines how NHS organisations and local authorities must provide care and support to individuals, including for the management of safeguarding issues. This includes using information to assess any person who appears to require care and support.

Children Act 1989
Sets out the duties of local authorities and voluntary organisations in relation to the protection and care of children. It requires organisations that come into contact with children to cooperate and share information to safeguard children at risk of significant harm.

Control of Patient Information Regulations 2002 (COPI)
Allows information to be shared for specific reasons in relation to health and care, such as for the detection and prevention of cancer, to manage infectious diseases, such measles or COVID-19. It also allows for information to be shared where support has been given for research or by the Secretary of State for Health and Social Care.

Coroners and Justice Act 2009
Sets out that health and care organisations must pass on information to coroners in England.

Employment Rights Act 1996
Sets out requirements for employers in relation to their employees. This includes keeping records of staff when working for them.

Equality Act 2010
Protects people from discrimination based on their age, disability, gender reassignment, pregnancy or maternity, race, religion or belief, sex, sexual orientation. Organisations may need to use this information to ensure that they are complying with their responsibilities under this Act.

Female Genital Mutilation Act 2003
Requires health and care professionals to report known cases of female genital mutilation to the police.

Fraud Act 2006
Defines fraudulent activities and how information may be shared, for example with the police, to prevent and detect fraud.

Health and Social Care Act 2008 and 2012
Sets out the structure of the health and social care system and describes the roles of different types of organisations. It sets out what they can and can't do and how they can or can't use information. It includes a duty for health and care staff to share information for individual care, unless health and organisations have a reasonable belief that you would object. In addition, health and care organisations may need to provide information to:

- The Secretary of State for Health and Social Care
- NHS England, which leads the NHS in England and provides information, data and IT systems for health and social care
- The Care Quality Commission, which inspects health and care services
- The National Institute for Health and Care Excellence (NICE), which provides national guidance and advice to improve health and care

Health and Social Care (Community Health and Standards) Act 2003
Allows those responsible for planning health and care services to investigate complaints about health and care organisations they have a contract with.

Health Protection (Notification) Regulations 2010
Requires health professionals to help manage the outbreaks of infection by reporting certain contagious diseases to local authorities and to the UK Health Security Agency. The UK Health Security Agency is responsible for protecting people from the impact of infectious diseases.

Human Fertilisation and Embryology Act 1990
Requires health organisations to report information about assisted reproduction and fertility treatments to the Human Fertilisation and Embryology Authority.

Human Tissue Act 2004
Requires health organisations to report information about transplants, including adverse reactions to the Human Tissue Authority.

Inquiries Act 2005
Sets out requirements in relation to public inquiries, such as the UK COVID-19 Inquiry. Public inquiries can request information from organisations to help them to complete their inquiry.

Local Government Act 1972
Sets out the responsibilities of local authorities in relation to social care including managing care records appropriately. For example, it lays out how they should be created, stored and how long they should be kept for.

NHS Act 2006
Sets out what NHS organisations can and can't do and how they can or can't use information. It allows confidential patient information to be used in specific circumstances for purposes beyond individual care. These include a limited number of approved research and planning purposes (see Control of Patient Information Regulations 2002 (COPI) above). Information can only be used where it is not possible to use information which doesn't identify you, or where seeking your explicit consent to use the information is not practical. The Act also sets out that information must be shared for the prevention and detection of fraud in the NHS.

Public Records Act 1958
Defines all records created by the NHS or local authorities as public records. This includes where organisations create records on behalf of the NHS or local authorities These records therefore need to be kept for certain periods of time, including permanently in some cases.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
Requires employers to report deaths, major injuries and accidents to the Health and Safety Executive, the national regulator for workplace health and safety.

Safeguarding Vulnerable Groups Act 2006
Sets out requirements for organisations who work with vulnerable to share information and to perform pre-employment checks with the Disclosure and Barring Service (DBS), which is responsible for helping employers make safer recruitment decisions.

Statistics and Registration Service Act 2007
Allows health organisations that plan services and local authorities to receive and disclose health and care information to the Office for National Statistics (ONS). The ONS is the UK's largest independent producer of official statistics.

Terrorism Act 2000 and Terrorism Prevention and Investigation Measures Act 2011
Requires any person to share information with the police for the prevention and detection of terrorism related crimes.

The Road Traffic Act 1988
Requires any person to provide information to the police when requested to help identify a driver alleged to have committed a traffic offence.