

Context

NHS England have issued a DPN that legally requires GP Practices to provide the OpenSAFELY Data Analytics Service Pilot with access to pseudonymised GP patient data for studies beyond COVID-19.

The full pseudonymised GP data processed by the service contains structured and coded data only. It does not contain free text or information such as letters, images, and correspondence. Type 1 Opt-out is applied by default for all studies approved to use the service. The National Data Opt-out will be applied on a study specific basis.

The DPN applies to TPP (SystemOne) and Optum (EMISWeb) practices only. (Medicus practices are out of scope). Practices have 6 weeks from the date of the DPN to review and accept it.

What does the practice need to do?

There are four actions practices need to complete, to comply with the DPN. An action summary and estimated time to complete is tabled below.

#	Action	Estimated time
1	Instruct your system supplier via the clinical system <i>(From within SystemOne or EMISWeb)</i>	2mins
2	Update the practice's Privacy Notice <i>(Use NHSE's prepared content or develop your own)</i>	3mins – 20mins
3	Complete DPIA <i>(Use NHSE's pre-worked template, adapt it or complete your own)</i>	5mins – 45mins
4	Update practice's 'Register of Processing Activities' or 'Information Asset Register' ...of data flows from DPIA	5mins
Time Summary		
Using pre-prepared materials from NHS England		15mins
Using own materials		+1hr

The detailed action sheet is on page 2.

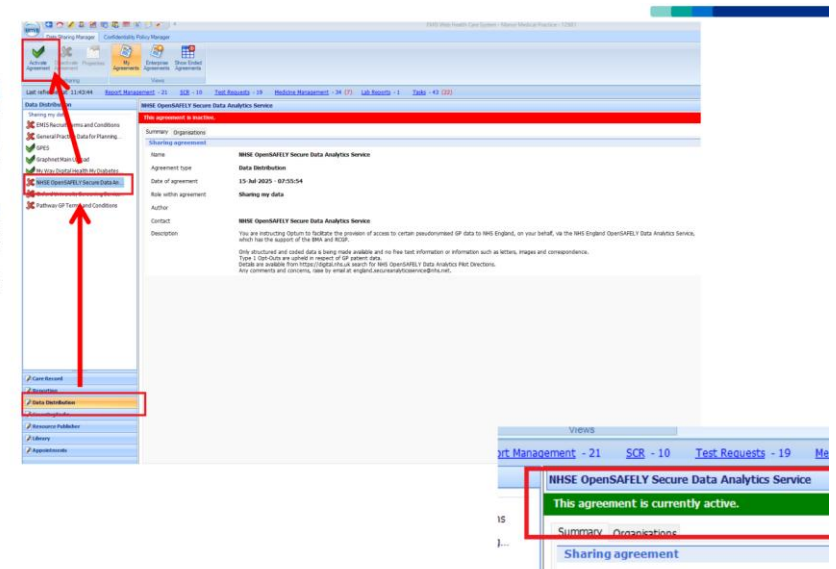
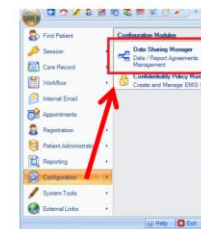
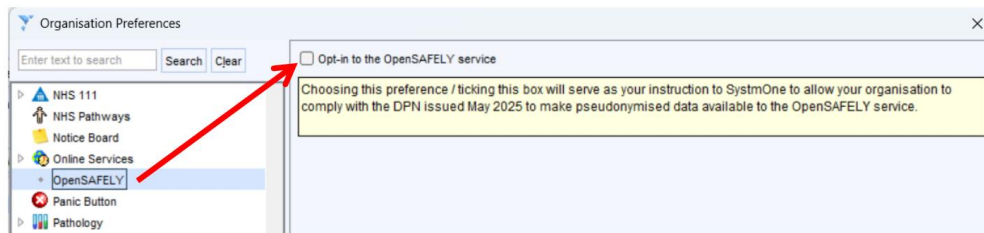
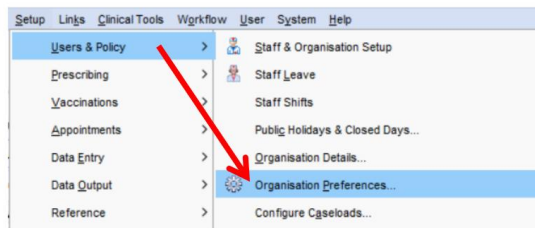
ACTIONS

1. Instruct your clinical system supplier to make GP data available to the service.

Practices can instruct their clinical system supplier from within SystmOne or EMISWeb.

EMISWeb	Configuration → Data Sharing Module and search for “NHS England OpenSAFELY Data Analytics Service”
SystmOne	Setup → Users & Policies → Organisation Preferences → OpenSAFELY (or use search bar)

- TPP and Optum will provide regular reports to NHS England; this will help NHS England to support practices to meet their legal obligation of complying with the DPN.
- The collection and sharing of these reports with NHS England, has the support of the BMA and RCGP representatives of the Joint GP IT Committee.



2. Update the practice's privacy notice.

NHS England have provided the below text to explain the processing of data for this service. Practices can add this to their own privacy notices or draft their own information.

“NHS England has been directed by the government to establish and operate the OpenSAFELY COVID-19 Service and the OpenSAFELY Data Analytics Service. These services provide a secure environment that supports research, clinical audit, service evaluation and health surveillance for COVID-19 and other purposes.

“Each GP practice remains the controller of its own GP patient data but is required to let approved users run queries on pseudonymised patient data. This means identifiers are removed and replaced with a pseudonym.

“Only approved users are allowed to run these queries, and they will not be able to access information that directly or indirectly identifies individuals.

“Patients who do not wish for their data to be used as part of this process can register a type 1 opt out with their GP.

You can find additional information about OpenSAFELY at <https://www.opensafely.org/>”

3. Review the draft Data Protection Impact Assessment

Weblink: [\(DPIA\) for the OpenSAFELY Data Analytics Service](#)

A pre-populated template has been provided by NHS England for practices to cover their role as controller of the pseudonymised dataset. Practices may choose to use or adapt this DPIA, or develop their own. They may wish to seek advice from their DPO regarding this.

4. Update the practice's 'Record of Processing Activity' or 'Information Assets Register'

Practices are encouraged to review the below wording before updating their registers.

- OpenSAFELY is a secure platform that enables approved users to run queries on pseudonymised GP and NHSE patient data for research and planning purposes without the patient identifiable data being seen or accessed.
- The GP data resides in the GP system suppliers (GPSS) data estate (sometimes referred to as “boundary”).
- The GP data is pseudonymised by the GPSSs. NHS England's (NHSE) pseudonymised data is shared with the GP System Suppliers to hold in their secure data estate, under agreement via data processing agreements held directly with the GPSSs.
- The NHSE data is linked with the pseudonymised GP data and is queried. The results (of the query) are processed within the GP System Supplier's secure environment. At point of query, NHSE becomes the data controller for the linked results, as per the Direction and DPN.
- The results (outputs) are presented as aggregated data with small number suppression, no patient identifiable data is transferred or disclosed.

Last updated 20 August 2025

Key Points

- There is no transfer or flow of GP data to the outside the GP System Supplier's data centres (also referred to as boundary).
- No pseudonymised data is accessed outside of the GP System Supplier's boundary.
- Any outputs from the OpenSAFELY service are aggregated and/or anonymous.
- Under the DPN, the GP Practice is giving permission to allow the remote querying of its data (held by the GP System Suppliers) for the Purposes set out in the Direction by NHSE; this is not sharing of data.

Legal basis for processing the data

For the data analytics service, the data will be processed under the legal basis provided under the OpenSAFELY Data Analytics Service Pilot Directions 2025 and its associated data provision notice (DPN).

- UK GDPR Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject (the DPN).
- 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 DPN supplemented by: Data Protection Act 2018 basis which is Data Protection Act 2018 (DPA 2018) Schedule 1, Part 2, paragraph 6: Statutory etc and government purposes.
- Under the common law duty of confidentiality, legal requirements as GP Practices are required by law to process and share the data identified in the DPN with NHS England.

The service will be delivered under the [OpenSAFELY Data Analytics Directions 2025](#) until 31 March 2027.

For each study submitted to access the Service: NHS England must consult with the BMA and RCGP for advice and NHS England must consult with the NHS England Advisory Group for Data. The types of studies permitted; i) Clinical Audit, ii) Service Evaluation, iii) Health Surveillance, iv) Research and two new types of studies, v) Health & Social care policy, planning and commissioning and public health purposes (following the support of each nominated representatives from the BMA and RCGP, and a representative from NHSE and DHSC) and vi) Evaluation of the Service.

GP practices remain the controller for the pseudonymised GP patients records, in the same way as they are for the data they input into their clinical systems. Through the DPN, GP practices give NHS England permission to remotely query that data and to do essential technical work to Supporting practices to meet legal obligation of the OpenSAFELY Data Analytics Service DPN

Last updated 20 August 2025

keep it safe and effective. Once the pseudonymised GP data is queried, and potentially linked to other NHS England datasets, NHS England rather than the GP practice becomes the controller for the linked pseudonymised dataset. This dataset never leaves the system supplier boundary and is not accessed by approved users. Approved users use these smaller, linked datasets to run other remote queries and return anonymised, aggregate results.

NHS England have additional [FAQs](#) and a dedicated mailbox for advice, comments, questions or concerns.

Email to: england.secureanalyticsservice@nhs.net

List of resources and weblinks

Resource Name	Weblink
1 Directions Letter & Requirements Specification	https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/nhs-opensafely-data-analytics-service-pilot-directions-2025
2 Data Processing Notice (DPN)	https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/data-provision-notices-dpns/opensafely-data-analytics-service
3 Privacy Notice	https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/nhs-opensafely-data-analytics-service-pilot-directions-2025/nhs-opensafely-privacy-notice
4a NHSE Data Protection Impact Assessment (DPIA)	https://digital.nhs.uk/binaries/content/assets/website-assets/corporate-information/directions-and-data-provision-notices/data-provision-notices/opensafely-data-analytics-service-pilot/nhs-england-opensafely-analytics-service-pilot-dpia-v1.0.1.pdf
4b GP DPIA Template (pre-populated)	https://transform.england.nhs.uk/documents/189/20250722_GP_Data_Protection_Impact_Assessment_Template.docx
5 IG Portal, OpenSAFELY FAQs	https://transform.england.nhs.uk/information-governance/frequently-asked-questions/#questions-about-opensafely
6 Further help and support, dedicated mailbox	england.secureanalyticsservice@nhs.net
7 OpenSAFELY Website	https://www.opensafely.org/