hscic Health & Social Care Information Centre

Annex A - HSCIC Data Access Requests and Associated Governance

Data Sharing Framework Contract (DSFC)

A Data Sharing Framework Contract (DSFC) must be agreed between the Health and Social Care Information Centre (HSCIC) and an organisation acting as a data controller, such as a CCG, in order to disseminate data either directly or via a Data Services for Commissioners Regional Office (DSCRO). However data cannot be shared under a DSFC alone; a Data Sharing Agreement specific to the request is required for that.

The DSFC is an over-arching document that specifies the basis for data to be shared and outlines the terms and conditions of how data must be managed once it has been released to the data controller.

Data Sharing Agreements (DSAs)

Data Sharing Agreements (DSAs) are additional documents that specify: the type of data being released, the purposes for which the data will be used, any specific Terms and Conditions of use and details relating to the security of the data.
These apply to data controllers, including any work undertaken by data processors who are contracted to perform services on behalf of an organisation.

Where an organisation is receiving data on a CCG's behalf, this organisation is acting as a data processor for that CCG. The CCG is the data controller ultimately responsible for the safety and security of that data.

Every CCG must have a DSFC with the HSCIC as well as DSAs in place for data to flow. DSAs cannot be approved without the existence of a DSFC. The HSCIC Data Access Request Service (DARS) manages this process. Relevant s251 approval is needed if an identifier (e.g. NHS number) is to flow.

Formalising a DSA

A Data Access Request Service (DARS) application must be completed and submitted by the organisation requesting the data (e.g. CCG), to formalise a DSA.

This is reviewed by the Data Access Advisory Group (DAAG) to ensure that the use of patient data for improving patient care processes and/or research purposes is controlled and the risk of disclosure is minimised.

When the DAAG is satisfied that there is a legitimate legal basis and requirement for the data and that dissemination is appropriate, a DARS application is recommended for approval by DAAG and passed to the Senior Information Risk Owner (SIRO) who makes the final decision on behalf of HSCIC Board. If approval is given, this triggers the creation of a Data Sharing Agreement (DSA). This is signed by a number of parties including the CCG's Caldicott Guardian. Data must not flow unless a DSA is in place to underpin that data release.

Specifically in relation to commissioner applications to receive data, the following purposes require a DARS application (resulting in a DSA):

- Risk Stratification requests
- Invoice Validation requests
- Stage One Accredited Safe Haven requests
- Pseudonymised data requests

Any dataset released by a DSCRO to a commissioning organisation should be included in these applications.

How does the DARS process protect data?

The HSCIC's decisions and actions are bound by law and policies and the organisation checks that there is an appropriate legal basis to receive, process and flow data to a CCG. The HSCIC also checks that CCGs have safeguards in place to store and handle the data safely and securely. Each request for data, other than for aggregate (where small numbers are suppressed) or anonymised data [see Summary of Terms below], is evaluated by the Data Access Advisory Group (DAAG).

It is paramount that all CCGs have DSAs in place to prevent data release from ceasing. Recipients of data are being audited and these audit reports are made public

It is also important that, when a data processor or any other arrangements change, an amendment to an existing DSA is submitted to the HSCIC to ensure that coverage is accurate and representative of the use of data that the data controller is responsible for.

Further information about the Data Access Request Service (DARS) process and data sharing can be found here.

All DSFC forms and DARS applications should be submitted to enquiries@hscic.gov.uk. If you require additional clarification, please do not hesitate to contact the HSCIC using this address, quoting 'Commissioning DARS application enquiry' in the subject title.

Summary of terms:

Term	Description
Aggregated Data:	Statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.
Anonymised Data:	Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place.
Data Controller:	A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. In relation to data sharing for commissioning, HSCIC is the data controller until this data is released at the request of a commissioner. Once released, the CCG becomes the data controller.
Data Processor:	A person who (either alone or jointly or in common with other persons) process Data as is necessary to perform its obligations under Agreement and only in accordance with any instruction given by the Data Controller E.g. a Commissioning Support Unit or third party processor
De-identified Data:	This refers to personal confidential data, which has been through anonymisation in a manner conforming to the ICO Anonymisation code of practice. There are two categories of de-identified data: • ***De-identified data for limited access:*** this is deemed to have a high risk of re-identification if published, but a low risk if held in an accredited safe haven and subject to contractual protection to prevent re-identification. • ***Anonymised data for publication:*** this is deemed to have a low risk of re-identification, enabling publication.
DSFC:	A Data Sharing Framework Contract (DSFC) forms part of the safeguards the HSCIC uses to ensure that high standards are

	maintained by the organisations we provide information to. It is used in conjunction with the Agreement. A Contract lets customers know what their responsibilities are in relation to information received from the HSCIC. Each release of data to a customer is then covered by a separate Data Sharing Agreement. The maximum duration for a DSFC is currently 3 years.
DARS:	The HSCIC service responsible for receiving and processing applications for data.
DARS application:	A Data Access Request Service (DARS) application is an application submitted by a requesting organisation (e.g. CCG) setting out the nature of the requested data and the purpose for which it is being requested. The maximum duration for a DSA is currently 12 months. (A renewal application is required in the event that an organisation wishes to continue this DSA.)
DAAG*:	The Data Access Advisory Group (DAAG) is a committee who review DARS applications to ensure that the use of patient data for improving patient care and for research purposes is done in a controlled environment where any risk of disclosure is minimised. Where DAAG are satisfied, a DARS application is recommended for approval which triggers the population of a Data Sharing Agreement (DSA).
DSA:	The Data Sharing Agreement (DSA) covers what type of data is being released, the purpose it will be used for and any further specific conditions E.g. any further sharing of data. A Data Sharing Agreement is formulated once a DARS application has been to DAAG for approval.
Fair Processing Notice:	The oral or written statement that individuals are given when information about them is collected is called a 'fair processing notice', or as per recent guidance issued by the Information Commissioner's Office (ICO) a 'privacy notice'. The ICO website provides further detailed guidance on what should be included.
Pseudonymisation:	The process of distinguishing individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity.
Pseudonymised Data:	Data in a form that distinguishes individuals in a dataset by using a unique identifier which does not reveal their 'real world' identity.
Re-identification:	The process of analysing data or combining it with other data with the result that individuals become identifiable. Sometimes termed 'de-anonymisation'.

*Shortly to be replaced by IGARD (Independent Group Advising on Release of Data)