# DATA SHARING AGREEMENT (DSA)

# CHECKLIST

**This Checklist is guidance only.**

**There may be other considerations/processes and documents that you may have to take into account or have in place to fully comply with all the requirements of the retained EU law version of the General Data Protection Regulation ((*EU) 2016/679*) ("UK GDPR"), the Data Protection Act 2018 (DPA 2018) and any other relevant data protection legislation.**

**We strongly suggest that you liaise with your Data Protection Officer (DPO) and other parties to the DSA, including taking legal advice where appropriate to ensure that you are compliant with UK GDPR/DPA 2018 and any other relevant data protection legislation.**

## 1. PURPOSE AND OBJECTIVES

Ensure that the DSA has a clearly defined purpose and/or objective. This means it should be clear why the DSA is being put into place and what the intention is behind the information sharing. This effectively will set the context of the structure and service and make it clear as to why the DSA is necessary.

## 2. INDENTIFY THE TYPES OF INFORMATION TO BE SHARED/ACCESSED

The type of information to be shared must be clear. So, if it is special category data this needs to be clear. The DSA should have a list of the type of information such as:

- Name, address, NHS number and phone number
- Medical Conditions
- Treatment provided and contact the patient has had with the organisation
- Care Plans
- Emergency department treatment
- Discharge Summaries
- Medication Reviews
- Medical Reports
- Results of investigations, such as x-rays, scans, and laboratory tests.

Note that even if the data to be shared is anonymised or pseudo-anonymised, it should still be mentioned in the DSA.

## 3. WHO IS GAINING ACCESS TO THE INFORMATION

It should be clear who is gaining access to the information. For example: healthcare professionals from certain organisations, hospital trusts, CCG etc and identify the type of information each party will gain access to. It may be that the CCG only has access to pseudo-anonymised information, if so, the DSA should state this and make it clear that that information will never be identifiable. Also state the purpose e.g. audit.

## 4. SET OUT THE LAW AND LEGAL OBLIGATIONS

Make sure that the correct laws are stated in the document so it is clear what legislation, standards, codes of practice and guidance apply e.g.

- The retained EU law version of the General Data Protection Regulation ((*EU) 2016/679*) ("UK GDPR") (ensure Article 6 and 9 are met), and the Data Protection Act 2018 (DPA 2018)
- Common Law Duty of Confidentiality
- Freedom of Information Act 2000
- Human Rights Act 1998 (Article 8)
- Mental Health Act 1983
- Mental Capacity Act 2005
- GMC Guidance – Confidentiality: good practice in handling patient information
- HSCIC Guide to Confidentiality 2013 as complemented by the HSCIC Code of practice on confidential information December 2014
- Information Governance/Caldicott 3 Review: 'Information: To Share or Not to Share? The Information Governance Review
- Records Management Code of Practice for Health and Social Care 2016
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- NHS England Safe Haven Procedure
- NHS Constitution for England
- Information Security Management: NHS Code of Practice
- ICO Data Sharing Code of Practice
- Published Privacy Notices as applicable to Parties to this DSA
- Data Security & Protection Toolkit (DSPT)

## 5. LAWFUL BASIS AND SPECIAL CATEGORY CONDITIONS

It is very important that the DSA sets out the correct lawful basis and special category conditions under the UK GDPR as well as the relevant Schedule 1 condition of the DPA 2018 that the parties to the DSA are relying upon in order to process information. There may be a number of these and most DSA's identify the categories that may apply and are relied upon. Note these will depend upon the nature of the processing and who is processing and for what purpose. If processing involves sharing identifiable healthcare data then that will be classed as special category data and may require the parties to establish a relevant special category condition. NOTE: that consent is not always required for certain types of processing, but where consent is required e.g. at point of contact, it should be made clear in the DSA.

## 6. START DATE AND REVIEW DATE

The start date and review dates of the DSA should be clearly set out. This establishes when the DSA comes into effect, but more importantly a review date also evidences good practice in that the parties agree to review in the event that there are any changes or amendments that need to be made in line with current law or changes to processing.

## 7. PARTIES

Parties to the agreement (including organisations), should be clearly listed and each party should sign the agreement. Avoid documents that try to cover a number of different services (which are either identified or to be identified in the future). A DSA should be clear and valid in respect of current services to be delivered and information that is going to be imminently processed. It is bad practice to have a document that tries to be a "catch all" to prevent parties having to re-sign at a later date when services are defined.

**NOTE:**

**Ensure that you have dealt with the following items where necessary and relevant:**

- ☐ **Update Privacy Notices**
- ☐ **Make sure all necessary data maps to assess flow of data are completed**
- ☐ **Ensure a Data Protection Impact Assessment (DPIA) has been carried out**
- ☐ **Check that any other agreements are in place or will be put into place (e.g. service level agreements)**
- ☐ **Liaise with and ensure you have signed off with the DPO of any public body involved or other DPO**