

Sharing Personal Data – BHBIA Quick Guide February 2021

This guide summarises the latest guidance and support available when sharing personal data between data controllers.

In December 2020 two documents were issued that will help BHBIA members to take into account data protection requirements when sharing personal data with another organisation. In situations such as, when the commissioning end client is a data controller as is the:

- Data analytics agency/consultancy and the end client provides access to end client gathered doctor data for CRM purposes.
- MR agency and the end client provides the MR agency with a list of individuals for sampling.
- MR agency and non-anonymised film footage of MR participants is shared with the end client.

NHSX Data Sharing Agreement Template

The NHSX* issued a controller to controller 'Data Sharing Agreement (DSA) Template'. The template is designed to provide a high-level summary of data sharing between the parties signed up to the DSA.

<https://www.nhsx.nhs.uk/information-governance/guidance/data-sharing-agreement-template/>

There is also guidance on what the different sections of the template are designed to do. Whilst it has not been developed with business intelligence in mind it could be useful to BHBIA members sharing personal data; at the very least it acts as a prompt to for all the issues to be considered when data sharing. Do bear in mind though that a DSA is not legally binding; if enforceable rights are required, then these need to be framed in a Data Processing Agreement, rather than a DSA.

* NHSX is a joint unit bringing together teams from the Department of Health and Social Care and NHS England and NHS Improvement to drive the digital transformation of care.

ICO Data Sharing Code of Practice

The UK Information Commissioner's Office (ICO) launched a statutory Data Sharing Code of Practice:

“to give individuals, businesses and organisations the confidence to share data in a fair, safe and transparent way in this changing landscape. This code will guide practitioners through the practical steps they need to take to share data while protecting people’s privacy.”

<https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/>

The Data Sharing Code contains practical guidance on how to share personal data fairly and lawfully, and how to meet your accountability obligations. It does not impose any new conditions on data sharing, but will help you comply with your legal obligations under the UK GDPR and the DPA 2018. Data protection law is an enabler for fair and proportionate data sharing, rather than a blocker.

The code is mainly aimed at organisations that are controllers sharing personal data. Data sharing with a processor or within organisations is not covered by the code.

Data sharing includes

“the disclosure of personal data by transmission, dissemination or otherwise making it available”.

This includes:

- providing personal data to a third party, by whatever means;
- receiving personal data as a joint participant in a data sharing arrangement;
- the two-way transmission of personal data;
- and providing a third party with access to personal data on or via your IT systems.

We have reproduced key parts of the ICO’s Data Sharing Code below but we suggest you familiarise yourself with the full Code and use it to check the detail.

Deciding to share data

We recommend that as a first step you carry out a Data Protection Impact Assessment (DPIA), even if you are not legally obliged to. A DPIA will help you assess the risks in your planned data sharing and determine whether you need to introduce any safeguards. This will also help to provide reassurance to those whose data you plan to share. Do remember you must carry out a DPIA for data sharing that is likely to result in a high risk to individuals.

Data sharing agreements

It is good practice to have a data sharing agreement (DSA). Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities.

There is no set format for a DSA; it can take a variety of forms, depending on the scale and complexity of the data sharing. You should address a range of questions in your DSA:

- Who are the parties to the agreement?
- What is the purpose of the data sharing initiative?
- Are we sharing data along with another controller?
- Which other organisations will be involved in the data sharing?
- What data items are we going to share?
- What is our lawful basis for sharing?
- Is there any special category data, sensitive data or criminal offence data?
- What about access and individual rights?
- What information governance arrangements should we have?
- What further details should we include? E.g. a data sharing request form

Accountability

Accountability obligations mean that if you are involved in a data sharing arrangement, you are responsible for your compliance with the GDPR or DPA 2018, and you must be able to demonstrate that compliance. There is a general obligation to evidence your compliance and justify your approach, so you should maintain relevant documentation and adopt additional measures as necessary. If you have a DPO (data protection officer) they should be closely involved from the outset in any plans to enter into a data sharing arrangement.

Fairness and transparency in data sharing

Always to share personal data fairly and in a transparent manner. When you share personal data, you must ensure it is reasonable and proportionate. You must treat individuals fairly and not use their data in ways that would have unjustified adverse effects on them. Before sharing data, you must tell individuals about what you propose to do with their personal data in a way that is accessible and easy to understand.

Lawfulness

As well as making sure that you have a lawful basis for sharing personal data you should be aware of laws other than data protection law that could constrain your ability to share data e.g. copyright restrictions.

Lawful basis for sharing personal data

You must identify at least one lawful basis for sharing data before you start. You must be able to show that you considered this before sharing any data, satisfy the accountability principle.

Security

Data protection law requires you to process personal data securely, with appropriate organisational and technical measures in place.

The rights of individuals

In a data sharing arrangement, you must have policies and procedures that allow data subjects to exercise their individual rights easily. There are additional requirements if your data sharing involves automated decision-making.

Sharing personal data in databases and lists

The transfer of databases or lists of individuals is a form of data sharing. It is your responsibility to satisfy yourself about the integrity of the data supplied to you.

You should make appropriate enquiries and checks, including the following:

- confirm the source of the data;
- identify the lawful basis on which it was obtained and that any conditions attached;
- check what individuals were told at the time of handing over their data;
- verify details of how and when the data was initially collected;
- check the records of consent, if you are relying on consent;
- review a copy of the privacy information given at the time of collection of the data;
- check what information was given to individuals i.e. privacy information;
- check that the data is accurate and up to date;
- and ensure that the data you receive is not excessive or irrelevant for your needs.

In addition, you must tell data subjects who you are sharing their data with, and for what purposes. You must give privacy information to data subjects at the same time as collecting the data from them or within a reasonable period if the data has been shared with you indirectly.

It is good practice to have a written contract with the organisation supplying you with data.

Data sharing and children

If you are considering sharing children's personal data, you must take extra care. Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child. You should carry out a DPIA to assess and mitigate risks to the rights and freedoms of children, which arise from your data sharing.

Data sharing in an urgent situation or in an emergency

If carrying out MR with vulnerable individuals e.g. patients suffering from depression you should consult this section of the Code so that you are equipped with the right approach if you have to share relevant and proportionate information in an emergency e.g. the respondent appears to be at risk of suicide.

Annexes within the Code

A: Data sharing checklist providing a step-by-step guide to deciding whether to share personal data, highlighting what you should consider to make sure that your sharing complies with the law and meets expectations.

B: Data sharing request form template for use by the organisation making the request for data sharing.

C: Data sharing decision form template for use by the organisation taking the decision to share data.

Further Information

For further detail on all guidelines please see the BHBIA Legal & Ethical Guidelines for Healthcare Market Research at <https://www.bhbia.org.uk/guidelines-and-legislation/legal-and-ethical-guidelines>.

If you have any queries about this Quick Guide or the BHBIA Legal & Ethical Guidelines for Healthcare Market Research, please visit www.bhbia.org.uk and submit your query via 'My BHBIA'. Please note: this ad hoc advisory service is available to full BHBIA members only.

Prepared by the BHBIA's Ethics & Compliance Committee February 2021

The BHBIA's Ethics & Compliance Committee is providing this guidance as general information for its members. It is not legal advice and should not be relied upon as such. Specific legal advice should be taken in relation to any specific legal problems or matters. Whilst every reasonable effort is made to ensure the information is accurate, no responsibility for its accuracy or for any consequences of relying on it is assumed by the BHBIA.

British Healthcare Business Intelligence Association
Ground Floor, 4 Victoria Square, St. Albans, Herts AL1 3TF
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk

A Private Limited Company Registered in England and Wales