Data related regulations, Data Protection Impact Assessment and Data Sharing Agreement guidance for researchers

Contents

Scope of document

This document aims to explain GDPR (General Data Protection Regulation) terminology and cover GDPR requirements as applied to personal data that may be collected and used in research. It also covers the type of data sharing agreements (DSAs) and Data Protection Impact Assessments (DPIAs) that may be required.

1. What is personal data and when does GDPR apply

1.1 What is the GDPR and DPA 2018?

The GDPR is the General Data Protection Regulation (EU) 2016/679. It sets out the key principles, rights and obligations for most processing of **personal data** (see definition in section 1.2) but it does not apply to processing for law enforcement purposes, or to areas outside EU law such as national security or defence.

The GDPR is a European Regulation and automatically applied in the UK until the end of the transition period (31st of December 2020). After this date, it became UK law under the European Union (Withdrawal) Act 2018, with some technical changes to make it work effectively in a UK context.

The Data Protection Act 2018 (DPA) is the UK's implementation of the General Data Protection Regulation (GDPR). It updates and replaces the Data Protection Act 1998, and came into effect on 25 May 2018.

The DPA sits alongside the GDPR, and tailors how the GDPR applies in the UK, for example, by providing exemptions. It also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defence, and sets out the Information Commissioner's Office (ICO) functions and powers.

1.2 What is personal data?

Under the DPA, personal data means "information about a particular living individual", where that individual can be identified from the information, or by combining the details with other information. It doesn't apply to truly anonymised data.

Personal data is defined under the DPA as:

"data which relate to a living individual who can be identified:

(a) from those data,
or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."

Personal data must be about a living person, meaning that the DPA does not apply to mortality or other records about the deceased, although such data could still be protected by confidentiality or other legal rules.

1.3 The UK GDPR key principles

The GDPR Article 5 lists principles of processing personal data, and, we are required to ensure that personal data is:

Principle 1	used fairly, lawfully and transparently
Principle 2	collected for specified, explicit and legitimate purposes
Principle 3	adequate, relevant and limited to what is necessary for the purposes
Principle 4	accurate and, where necessary, kept up to date
Principle 5	kept in a form which permits identification of data subjects for no longer than is necessary for the purposes
Principle 6	kept secure with appropriate technical and organisational measures
Principle 7	handled responsibly

1.4 What is the difference between anonymised and pseudo anonymised data?

Anonymisation

According to the ICO, anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified. An individual may be directly identified from their name, address, postcode, telephone number, photograph, or if the person has a particular diagnosis or condition.

If an individual can be indirectly identified when certain information is linked together with other information, such as their place of work, job title, salary, their postcode (including the first part of the postcode), then this data is not truly anonymised.

Once data is truly anonymised and individuals are no longer identifiable, the data will not come under the scope of GDPR. For further information in regard to whether anonymisation is always necessary or possible, please refer to the ICO website. The UK Data Service can offer advice regarding anonymisation of datasets for archiving and sharing.

Pseudonymisation

Pseudonymisation is defined in the GDPR as "*the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual*" (Article 4(3b)).

Pseudonymised data falls under the scope of GDPR as certain identifiers could be collated to re-identify the person, for example a person's NHS number is a widely used pseudonym that should be considered as identifiable data.

Lesser used pseudonyms, such as a study ID, could be considered anonymised if there is certainty that any data recipient would be unable to reidentify the individual.

1.5 What is a link/identifying key?

To minimise the risk of accidental disclosure of personal data, it is advisable to create pseudonymised or, where possible, anonymised versions of working data for purposes of processing and analysis. The personal identifying information and the linked pseudonym IDs (key) are stored separately from a dataset in which individual identifiers have been replaced by the pseudonym IDs.

Please note that in the majority of cases, pseudonymised data will continue to be personal data as long as the identifying 'key' is held by the NHS site or Sponsor or a third party. If the link key is destroyed and the data does not contain direct/indirect identifiers, the data would be considered anonymised. If you are unsure whether your data is truly anonymised, please refer to the ICO website.

The identifying key is usually kept when it may be necessary to refer back to the original records for further information, or for verification, or if it is planned to provide feedback to participants or service providers. Anonymised data usually ensures confidentiality but prevents follow-up, verification or feedback and may not be compatible with the aims of the project.

1.6 What are special categories data?

Special category data includes information about an individual's:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and data concerning a person's **sexual orientation**.

Any personal data falling into these categories will need to be managed with extra care and should be collected only if this information is important to answer the research question. For research projects, if special categories data will be obtained, this needs to be clear in the Participant Information Sheet (PIS) and Consent form. The participant will need to explicitly consent to this information being collected.

1.7 What is the lawful basis for processing the Personal Data?

UK GDPR (Article 6) states that you must have a lawful basis for processing Personal Data. There are six available lawful bases for processing. No single basis is more important than the others and which basis is most appropriate to use will depend on your purpose and relationship with the participant. Further details in regards to each of the bases can be found on the HRA and ICO websites. One of the legal bases for processing data is consent. Even though consent is at the cornerstone of ethical research and can help manage expectations in terms of who has access to confidential information (common law of confidentiality), it is not likely to be your lawful basis to hold and process personal data for research purposes. For further explanation, please refer to the UK Research and Innovation and HRA websites. For research carried out at NHS Trusts and Universities, the lawful bases for processing Personal Data will most likely fall under "tasks being carried out in the public interest" for non-commercial studies and "legitimate interest" for commercial studies.

If you are processing special category data, an additional special category condition will need to be identified to comply with GDPR Article 9. For most studies, to comply with Article 9, the team will need to obtain explicit consent from the participant for the sensitive information to be collected. The UHBW Sponsor contact taking the study through sponsorship will ensure that the lawful basis

and special category condition (if applicable) for processing data is clear in the study documents (Protocol, IRAS form, PIS and ICF). Research Management Facilitators should refer to the latest guidance available in the HRA Approval Standards in regards to the legal basis that will be used for a study and the appropriate information that should be included in the study documents.

For research projects, how can I ensure that the Participant Information Sheet is compliant with the GDPR and ensure transparency?

Please refer to the HRA website which includes transparency wording for both Commercial and Non-commercial studies. The HRA website also provides examples of PISs/Consent forms for adult and children participants, including appropriate documentation for adults who may lack the capacity to consent.

2. How are Data Controllers and Data Processors defined and why does this matter?

The DPA draws a distinction between a 'data controller' and a 'data processor' to recognise that not all organisations involved in collecting, analysing and processing of personal data have the same degree of responsibility. All research involving processing of personal data must clearly define who are the data controllers and processors prior to the research commencing.

2.1 What is the difference between a data controller and a data processor?

It is the data controller that must exercise control over any processing of data and is responsible for ensuring that the GDPR is followed. Please note however, that a Data processor can be fined directly if they are not compliant with the GDPR.

Definitions taken from the ICO website	
Data controller	Means an organisation which (either alone or jointly or in common with another organisation) determines the purposes for which and the manner in which any personal data are, or are to be processed
Data processor	In relation to personal data, means any organisation which processes the data on behalf of the data controller.
The act of "processing"	In relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including a) organisation, adaptation or alteration of the information or data, b) retrieval, consultation or use of the information or data, c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

	d) alignment, combination, blocking, erasure or destruction of the information or data

The relevant research study agreements will detail which organisations are considered Data Controllers and Data Processors.

2.2 Determining whether an organisation is a data controller or processor

The data controller determines the **purposes** for which and the manner in which personal data is processed. It can do this either on its own or jointly with other organisations.

According to the ICO, for an organisation to be a data controller, they need to be the organisation deciding:

- to collect the personal data in the first place and the legal basis for doing so;
- which items of personal data to collect, i.e. the content of the data;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;
- whether subject access and other individuals' rights apply i.e. the application of exemptions; and
- how long to retain the data or whether to make non-routine amendments to the data.

The points mentioned above can be used to aid the decision on whether an organisation can be considered the data controller. Please note that a Controller may process data but they are doing so under their own account and not at the direction of another organisation. Whereas a processor is doing so under the direction of a Controller.

Please note that an organisation can be considered a data controller even if they do not hold the study link key or receive personal identifiable information. For example, for Commercial studies, the Commercial sponsor will be considered the data controller as they will determine the purposes for which and the way personal data is processed and in most cases, they will not be receiving identifiable information or hold the study key.

2.3 What are joint controllers?

The data controller exercises overall control over the '**why' and the 'how'** of a data processing activity. The definition provides flexibility and allows more than one organisation to be classed as a controller. For example, organisation A might mainly, but not exclusively, control the *purpose* of the processing with organisation B. Organisation B might then have some say in determining the purpose whilst being mainly responsible for controlling the *manner* of the processing.

These organisations could be classed as joint controllers if:

- They have a common objective regarding the processing
- They are processing data for the same purpose
- They are using the same set of personal data
- They designed the process together
- They have common information management rules

Obligations of joint controllers: The organisations will need to decide who will carry out which controller obligation under the GDPR. However, regardless of those arrangements, each controller remains responsible for complying with all the obligations of controllers under the GDPR.

Individuals' rights: In particular, the organisations must decide (and be transparent about) how they will comply with transparency obligations and individuals' rights. The organisation may choose to specify a central point of contact for individuals. However, individuals must remain able to exercise their rights against each controller.

2.4 Can a joint controller be held liable for non-compliance?

Yes. Individuals can seek compensation from joint controllers in exactly the same way as from any sole controller. Each joint controller will be liable for the entire damage caused by the processing, unless it can prove it is not in any way responsible for the event giving rise to the damage. The arrangement made between controllers is irrelevant for these purposes.

If as a joint controller you have had to pay compensation to an individual but were not wholly responsible for the damage, you may be able to claim back from another controller or processor the share of the compensation for which they were liable.

In addition, joint controllers are each fully accountable to supervisory authorities (such as the ICO) for failure to comply with their responsibilities. Further information can be found on the ICO website.

2.5 Can an organisation be a data controller and a data processor as well?

An organisation can be a controller and a processor of the same Personal Data, but they must be different Processing Activities (i.e. you are controller for one Processing Activity, because you are directing the purposes of the processing, and you are processor for another Processing Activity, because someone else is directing your use of the Personal Data). A controller may also process data but if they are directing the activity that would not make them a processor. Further information can be found on the ICO website.

For example: An NHS Trust is the Sponsor of the study (data controller). The Sponsor is working with a University Clinical Trials Unit (CTU) to manage the study on their behalf, the University CTU will very likely be acting as a data controller for the study duration. Once the study has finished, the CTU might still hold the study data, for example in a database (e.g REDCAP), therefore, in this instance the CTU would also act as the data processor as the data controller (Sponsor) will confirm how they process the data. Please note that this is a suggested example and the decision about which organisation will be act as a Data Controller/Processor will need to be reviewed for each trial as the activities being carried out may differ, and the University CTU may not act as a Data Controller for all studies.

2.6 If an organisation is sole processor and there are two or more joint controllers who does the processor take instructions from?

Where there is a joint controller relationship, a Data Sharing Agreement (DSA) will need to clearly set out each controller's roles and responsibilities, especially in relation to time-sensitive requests. Please refer to section 3.2 for further information about DSAs.

3. What agreements or other documents are necessary when personal data is being processed?

3.1 Data Protection Impact Assessments (DPIAs)

In accordance with the ICO, a DPIA is a process designed to help you systematically analyse, identify, and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations. DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects.

For UHBW sponsored studies, the Information Governance team (IG) have agreed that, if the research project has been through the HRA Approval process, a separate DPIA does not need to be completed. If, however, identifiable information needs to be sent to a country outside the EU/EEA, a DPIA may need to be completed. The R&I/IG UHBW teams will advise the research team whether this is required. Participating NHS organisations are not responsible for the DPIA of the processing activities that they will undertake on behalf of research Sponsors. It is the sponsor's responsibility to complete the DPIA for data processing.

For research tissue banks and research database studies that will not be reviewed by the HRA Approval team and where REC review is optional, a DPIA will need to be completed to ensure that the study complies with the relevant legislations.

For projects that are not classed as research, the IG team has advised that the project lead should consider completing a DPIA to ensure that the team complies with the GDPR. If you would like advice on whether a DPIA needs to be completed, please contact the IG team (InformationGovernance@uhbw.nhs.uk). If a DPIA is required, for audits please send a copy to the IG team and relevant Clinical Audit contact at UHBW, see http://www.uhbristol.nhs.uk/for-clinicians/clinicalaudit/

For lower and moderate risk projects, the DPIA can be signed by the IG team.

For high-risk projects, the DPIA will need to be signed by the ICO.

The IG team will facilitate this process. Please note that for research projects, the R&I team will work closely with the researcher to complete the DPIA and submit to it to IG.

A copy of the latest UHBW DPIA template can be found on the UHBW intranet on the information governance pages:
(http://connect/aboutus/CorporateGovernance/informationgovernance/Pages/IGResources.aspx)

3.2 Data sharing agreements

Where personal data is shared with individuals, companies, institutions or any other third parties to the Trust it will constitute a disclosure of the information from the Trust to another party. The Trust has a responsibility to ensure that personal data is shared securely and only with those who can evidence that they will also handle the data in line with all the above data protection principles. Contractual clauses will be included in contracts and/or data sharing agreements with collaborators or other third parties receiving personal data to ensure that the necessary due diligence can be evidenced. The purpose of these agreements is to set out the respective obligations and responsibilities between the parties.

There are a host of DSA templates that can be used and the choice of which one to use depends on the type of study and data transfer requirements:

1. The DSA included in the Organisation Information Document (OID) for non-commercial studies. This is used between the Sponsor and the participating site (between data controller and data processor)
2. The DSA included in the mNCA and mCTA agreements. These are used between the Sponsor and the participating site (between data controller and data processor)
3. The DSA included in the Participant identification centre (PIC) agreement. This is used between the NHS participating site and the PIC where the NHS participating site is the data controller and the PIC is the data processor.
4. The UHBW Standard DSA which can be used where there is collaborative approach to the project where information is either controlled by all organisations party to the agreement or where there may be multiple dataflows. This document can be used for joint controllers and can also be used as a tripartite agreement where there two joint controllers and a data processor. *The IG team will need to review this agreement before this is signed by all parties.*
5. The Standalone Processing Agreement can be used where UHBW is providing instructions to the 3rd party on what information is to be processed, how they are processing information and for what purpose. The processor must only act on UHBW's instructions. This document should be used as an addendum to a main contract or study protocol where no data

processing terms have been previously included. *The IG team will need to review this agreement before this is signed by all parties.*

6. The Bristol Health Partners Data Agreement, can be used for studies where there is a separate collaboration agreement between any of the Bristol Health Partners. This covers both controller-to-controller relationships and controller to processor arrangements by way of study specific schedules. The IG team has confirmed that they do not need to review this agreement but it should be signed off via R&I.

Please contact R&I if you need access to these templates.

Pseudonymisation describes the process where identifiable information is replaced with a unique code, for example a Study ID number. The Information Commissioner's Office considers data containing widely used pseudonyms, or pseudonymised data where an organisation holds the means to re-identify the individual, to be identifiable.

However, where a 3rd party does not hold the means to re-identify the individual, the pseudonym can be classed as non-identifiable. For example, a unique study ID with no other identifying factors being shared with a data processor would not always require a Data Sharing/Processing Agreement, but sharing NHS Number would require agreements to be in place.

4. Does GDPR apply to Audits and Service Evaluations?

Staff responsible for collecting personal data for the purposes of a clinical audit and/or a service evaluation will need to take responsibility for adhering to the GDPR principles and must ensure there are processes in place to handle potential data breaches. If data is rendered completely anonymous, GDPR regulations will not apply as the data is no longer considered personal data.

If the team is unsure whether their project is considered research/audit or a service evaluation, they should refer to the HRA website which includes a guidance document for defining research . The site also provides a decision tool to help project leads further.

Audits should be registered with and follow guidance of the UHBW's audit department. For projects that arer service improvements or evaluations, there is no specific department at UHBW, but these might be eligible for support and registration as a quality improvement (QI) project, see: http://connect/governanceandquality/QIHome/Pages/QIHome.aspx
. If a service evaluation project requires Patient Involvement, please contact the Patient Experience Team), and if necessary the UHBW Questionnaire, Interview and Survey (QIS) group. Teams undertaking audits or service evaluations (and any interviews or questionnaires done as part of these) should ensure that they have appropriate security arrangements in place to protect the personal data they hold, and ensure the data is destroyed when it is no longer required. The UHBW Information Governance team may require a Data Protection Impact Assessment to be performed (please refer to section 3 of this document). Please contact the relevant Service Manager or Clinical Lead to ensure the projects are undertaken in accordance with local procedures.

Please refer to the UHBW website for further information and contact details for undertaking patient surveys, interviews and focus groups.

5. Useful links

HRA/IRAS

http://www.hra-decisiontools.org.uk/research/ (HRA decision tool)

http://www.hra-decisiontools.org.uk/research/docs/DefiningResearchTable_Oct2017-1.pdf (HRA 'Defining research table')

https://s3.eu-west-2.amazonaws.com/www.hra.nhs.uk/media/documents/hra-approval-assessment-criteria-standards-document.pdf (link to HRA Approval standards)

https://www.hra.nhs.uk/approvals-amendments/what-approvals-do-i-need/confidentiality-advisory-group/ (HRA information about CAG)

ICO

https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/ (ICO- Further information about the DPA 2018)

https://ico.org.uk/media/1061/anonymisation-code.pdf (ICO - Further information about the process of anonymising data)

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (ICO – Lawful bases for processing personal data)

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (ICO – Further information for processing special category data)

Other useful links

https://digital.nhs.uk/coronavirus/coronavirus-data-services-updates/trusted-research-environment-service-for-england (NHS Digital - Further information about TREs)

https://www.healthdatagateway.org/ (Further information about access UK health datasets)

https://ukdataservice.ac.uk/learning-hub/research-data-management/#anonymisation (UK Data Service – Further information about anonymising data)

http://www.uhbristol.nhs.uk/research-innovation/for-researchers/is-it-research,-audit-or-service-evaluation/ (UHBW – Is my study considered research, audit or service evaluation?)