Adopters guidance

Complying with the UK GDPR Steps 1 - 7: an introduction

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Contents

Reviewed by: Health and Care IG Panel

If you are using personal data, you are obliged to protect it and comply with data protection law. The Information Commissioner's Office (ICO) is the UK regulator that oversees compliance and upholds information rights.

You can learn more about this in ICO's guide to the UK GDPR.

You should also consult your organisation's information governance team (advisers in data protection and confidentiality matters) early on when considering plans to adopt a technology.

Complying with the UK GDPR Steps 1 - 7: an introduction

Step 1: Register with ICO

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Reviewed by: Health and Care IG Panel

Every organisation or sole trader who processes personal data is legally required to register with ICO. Once you have registered, you will have to pay a data protection fee. This is used to fund ICO's work. If you do not pay the fee, you may be fined. ICO publishes the names of individuals and organisations who have paid the fee, and those fined for non-payment.

How to do it:

1. Use ICO's registration self-assessment to find out if you (as an individual or on behalf of your business or organisation) need to pay the data protection fee
2. Register on ICO's website and pay the data protection fee

Complying with the UK GDPR Steps 1 - 7: an introduction

Step 2: Consider doing a DPIA

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

Before you start processing health and care data involving the use of new technology, including in the context of deploying a technology in a health or social care setting, you should consider doing a DPIA. This will help you identify and minimise any data protection problems early on, and to fully consider the risks to patients and service users. It will also help you build public trust because it will help you consider how to make your data processing transparent (such as through creating privacy notices).

You can use the standardised DPIA template developed by the Health and Care IG Panel. It will also help you carry out the assessments required in steps 3 and 4 below.

A DPIA is required by law before you carry out processing of special category data on a large scale by an innovative technology, because this constitutes a high risk (see ICO's examples of processing 'likely to result in high risk'). Failure to carry one out when required could result in a fine, prosecution and damage to reputation.

You may need to modify the DPIA or create a new one at later stages of the technology adoption pathway if you change an existing processing activity. For example, if you make significant changes to how or why personal data is processed, or the type or amount of data being processed. In other words, a DPIA should be considered a 'live' document, started as early as possible and updated throughout the life of your project.

Learn how to do a DPIA and take a risk-based approach using ICO's guide to DPIAs, which includes an example template and practical checklists.

Also see the HRA's guidance on DPIAs for research. DPIAs for the processing of personal data that is done for the purpose of research are the responsibility of the sponsor.

In the context of technology adoption, doing a DPIA would normally be the responsibility of the relevant NHS or social care organisations in England and Wales.

Complying with the UK GDPR Steps 1 - 7: an introduction

Step 3: Determine if you are a data processor or controller

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

Controllers and processors are both responsible for complying with the UK GDPR. However, your obligations will vary in respect of each of the processing activities you carry out depending on whether you determine you are a controller or a processor for each processing purpose.

You must be able to demonstrate compliance with the data protection principles applicable to your role and take appropriate technical and organisational measures to make sure your processing is carried out in line with the UK GDPR.

You will be classed as a data controller for a processing activity if you:

- make decisions about what personal data is to be processed
- make decisions about how and why personal data is processed

If another party makes those decisions, they in turn will be a controller, and you will be their processor when you process personal data on their behalf. Data processors must select appropriate methods that meet the data controller's standards for data processing, as well as the standards defining what data is to be collected, why, and by which lawful basis under UK GDPR, the Data Protection Act, and Common law duty of confidentiality.

It is possible to be both a controller for one processing purpose, and a processor for a different purpose, within a single project. It depends on the facts, which you will need to assess. See examples in ICO's guidance on controllers and processors.

You may also determine that you and another organisation also both act as controllers of a processing activity (as joint controllers); for example, when you are processing personal data for a shared purpose.

Decision tool:

Use ICO's controllers and processors checklists to help determine whether you are a data controller or a data processor and describing the obligations under each role. Also see HRA's guidance on the role of research sponsors as controllers.

In the context of technology adoption, the relevant NHS or social care organisation in England and Wales would act as controller.

Complying with the UK GDPR Steps 1 - 7: an introduction

Step 4: Comply with article 6 and 9 of UK GDPR

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Overseen by: HRA (Health Research Authority)

Health and care data is considered personal data, and also special category data, under the UK GDPR. To comply with the law, therefore, you must identify:

1. a lawful basis for processing personal data under Article 6 of the UK GDPR, and
2. a separate condition for processing data special category under Article 9 of the UK GDPR

The lawful basis and condition you choose for your processing activities must be relevant and valid for each data processing situation. There are different types of bases/conditions that could be chosen, each with different requirements attached. You must make sure you can satisfy the relevant requirements if you rely on them. The different types are summarised below, along with guidance on the lawful basis/condition most relevant to adopters.

Article 6 of the UK GDPR

There are 6 lawful bases for processing personal data under Article 6 of the UK GDPR. At least 1 of these must apply whenever you process personal data, and you must determine in advance which one you are relying on and make this clear in your privacy notice. In the context of technology adoption, the legal basis of 'vital interests' will not apply.

Important note: if you want to process data for health or social care research, the ICO and the HRA strongly recommend that you do not use consent as your lawful basis. Instead, you should use 'task in the public interest' if your organisation has public powers (for example, universities, NHS organisations, Research Council institutes or other public authority). For private organisations (such as commercial companies and charitable research organisations), the processing of personal data for research should be done within 'legitimate interests'.

Get more information:

Read the HRA's guidance on consent in research and the legal basis for processing data.

Read ICO's guidance on the lawful basis for processing and how to apply legitimate interests in practice, including how to do a 'legitimate interests assessment'.

Use the HRA's templates with recommended wording to make sure your privacy notices and other information are consistent with the use of confidential patient and service-user information for research.

Article 9 of the UK GDPR

Health and care data is considered a type of special category data under UK GDPR. So, in addition to identifying a lawful basis as described above, you will also need to meet 1 of the 10 specific conditions in Article 9 of the UK GDPR. You should note that 5 of these require you to meet additional conditions and safeguards set out in UK law, in Schedule 1 of the DPA 2018. See ICO's guidance on special category data for full details.

In the context of technology adoption, you can rely on special condition Article 9(h) ('Health or social care (with a basis in law)') if the processing purpose is direct care. This is conditional on data being processed by a professional bound by a professional code and obligations of confidentiality or secrecy.

Important note: if you want to process data for health or social care research, whether processed by a public authority or by a commercial organisation or charitable research organisation, special category personal data should be processed under Article 9(2)(j) for research purposes, but only if processing such data is:

- necessary for archiving purposes, scientific or historical research purposes or statistical purposes
- subject to appropriate safeguards, and
- in the public interest

Get more information:

Read the HRA's guidance on safeguards and ICO's guidance on research provisions.

Complying with the UK GDPR Steps 1 - 7: an introduction

Step 5: Determine if your activities are research

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

During adoption of the technology, there could be various activities that could be considered research. See understanding the difference between research and non-research activities for more information.

If you will be doing research, including technology development activities, you need prior approvals from various organisations. These organisations include the Health Research Authority (HRA) and Health Care Research Wales (HCRW).

The HRA oversees responsible use of NHS health and (adult) social care data in research. It does this by providing the Research Ethics Service. This service is made up of many independent NHS Research Ethics Committees (RECs) that review health and social care research to provide ethics approval. The HRA also receives expert advice from the Confidentiality Advisory Group (CAG), an independent body that reviews applications for the use of confidential patient and service-user information for research (and non-research) uses. The HRA provides decisions based on this advice involving research, and issues approvals on behalf of the NHS for studies that are accessing data from NHS Trusts or GP practices.

More information:

- HRA Approval
- ICO's guidance on research provisions

Do you need research approval?

Read Is my study research? and Do I need NHS REC review? to help decide if you need approval from a REC. Even if you do not, you may still separately require approval from the HRA/HCRW.

Sometimes you may also need separate approval from the CAG, in addition to REC approval.

What approvals do I need?

If you plan to use data from NHS organisations for a research activity, you normally need to get approval from:

- a REC, and/or
- the HRA/HCRW (depending on whether your research will take place in England and/or Wales)

Important note: HRA/HCRW approval will be needed even if the data you will use has been rendered anonymous before use. You should apply for HRA/HCRW approval if the data is from NHS patients or staff and will be provided by an NHS organisation, or if NHS resources or staff will be involved in your research.

You need to obtain the **explicit consent** of an individual to receive confidential patient and service-user information about them for re-use in your research, if you are not part of their direct care team. When it can be demonstrated that obtaining consent is impossible (for example, because the individual has died without giving consent) or highly impractical in the situation, the information holder will need to make an application to CAG for a section 251 (NHS Act 2006) review to set aside the common law duty of confidentiality. If granted, this would provide a legal basis that allows you to receive this information for your research without consent.

Note that this type of consent (to have confidential information shared with you) is separate from UK GDPR consent. See the HRA's guidance on consent in research.

How to apply for research approvals

You can apply for HRA and HCRW approval, REC review and CAG review using the Integrated Research Application System (IRAS).

Being transparent with research

The HRA has a legal duty to promote research transparency. When applying for HRA and HCRW approval you should think about how you will share your findings and how you plan to involve patients and members of the public in the research. This is separate to recruiting patients and members of the public as research participants.

For practical resources and information about how to involve the public in research, read:

Make it public: transparency and openness in health and social care research

HRA's best practice in public involvement

Complying with the UK GDPR Steps 1 - 7: an introduction

Step 6: medical device clinical investigation approval

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

A clinical investigation of a technology is defined as research by the HRA and HCRW and needs approval. You will need to follow the steps described in step 5.

Clinical investigation of a non-CE or non-UKCA marked device

If you plan to do a clinical investigation for a non-CE or non-UKCA marked device, you will need approval from a REC.

How to get a medical device clinical investigation approval from a REC

Step A: Notify the MHRA

You must notify the Medicines and Healthcare products Regulatory Agency (MHRA) before you begin a clinical investigation.

Submit an MHRA devices application to the MHRA. When this is confirmed to be valid, you can submit your application for review on the HRA's Integrated Research Application System (IRAS). IRAS is a single system for applying for the permissions and approvals for health, social and community care research in the UK. The IRAS form explains what information you need to provide specifically for these types of investigations. See help and guidance on IRAS.

Email: mhracustomerservices@mhra.gov.uk with 'MHRA/HRA Coordinated assessment pathway' in the subject line.

Step B: Submit a REC application

Once the MHRA confirms your application as valid, you can submit your REC application on IRAS.

If confidential patient and service-user information is being processed without explicit (common law duty of confidentiality) consent then, as part of your application on IRAS, you will also need to apply to CAG (see further guidance on how to do this on IRAS).

CAG will provide independent advice to the HRA on whether your request for access to the confidential information should be approved based on its assessment criteria. Read

CAG's pre-application assessment before formal submission of an application, which will help you decide whether an application to CAG is an appropriate route.

Updates will be provided (including possible requests for additional information) and a possible meeting with the REC who will do the review. You will then be notified of the decisions, usually by the main email address you have provided and/or that of your sponsor representative.

Complying with the UK GDPR Steps 1 - 7: an introduction

Step 7: Follow the 8 Caldicott Principles

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

Follow the 8 Caldicott Principles that make sure people's information is kept confidential and used appropriately.

Caldicott Guardians help their organisations make sure confidential information about health and social care is used ethically, legally and appropriately. Caldicott Guardians should provide leadership and informed advice on complex matters involving the use and sharing of patient and service user confidential information, especially in situations where there may be areas of legal or ethical ambiguity.

For more information about the types of organisations that should have a Caldicott Guardian, see the National Data Guardian guidance on appointment of Caldicott Guardians. If your organisation does not have a Caldicott Guardian, you can contact the UK Caldicott Guardian Council: ukcgcsecretariat@nhs.net.

Important note: if you originally collected the data but you did so on the basis of UK GDPR consent, you would normally need to get new consent before you repurposed the data. This is to make sure your new processing is fair and lawful. You also need to update your privacy information to make sure that your processing is still transparent.

Get more information:

Read about purpose limitation in ICO's guide to the GDPR, and see ICO's guidance on research provisions.

