Developers guidance

How to comply with the UK GDPR as a developer

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: 20 January 2023

Contents

Reviewed by: Health and Care IG Panel

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

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

There are 8 steps to follow to comply with the UK GDPR.

How to comply with the UK GDPR as a developer

Step 1: Register with the ICO

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Every organisation or sole trader who processes personal data is legally required to register with the ICO. Once you have registered, you will have to pay a data protection fee. This is used to fund the ICO's work.

If you do not pay the fee, you may be fined. The ICO publishes the names of individuals and organisations who have paid the fee, and those fined for non-payment.

1. **How to do it:**
   Use the 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 the ICO website and pay the data protection fee

How to comply with the UK GDPR as a developer

Step 2: Do a data protection impact assessment (DPIA)

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

Before you start processing health and care data or deploying a technology in a health or social care setting, you should consider carrying out 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 the 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 should also consider the risks of any additional new data-processing activity you later add to your project, before any data processing begins.

You may need to modify the DPIA or create a new one at later stages of the technology development 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 the ICO's guide to DPIAs, which includes an example template and practical checklists. The HRA has also published guidance on DPIAs for research.

How to comply with the UK GDPR as a developer

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

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

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 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. 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. See examples in ICO's guidance on controllers and processors.

Decision tool:

Use the ICO's controllers and processors checklists to help determine whether you are a data controller or a data processor. The descriptions of the obligations are listed under each role. The HRA has also published guidance on the role of research sponsors as controllers.

How to comply with the UK GDPR as a developer

Step 4: Have a lawful (also known as 'legal') basis for processing health data

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

Identifiable health data is considered personal data, and also special category data, under the UK GDPR. There are different sets of requirements for both. To process health data, you must identify:

1. a lawful basis under Article 6 of the UK GDPR
2. a separate condition for processing special category data 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 listed here (a) to f)). 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 development, the legal basis of 'vital interests' (Article 6(d)) 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 the 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'.

The HRA provides templates with recommended wording that health organisations should use to make sure their privacy notices and other information are consistent with the use of confidential patient 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 the ICO's guidance on special category data that describes these in detail.

Whether processed by a public authority or by a commercial organisation or charitable research organisation, special category personal data can 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 the ICO's guidance for research provisions within the UK GDPR.

How to comply with the UK GDPR as a developer

Step 5: Getting research approvals, if needed

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

Throughout the development of your technology, there could be various activities that could be considered research. Research in this context means any activity involving health and care data when your intention is to 'attempt to derive generalisable or transferable new knowledge to answer or refine relevant questions with scientifically sound methods'. National Clinical Audits of practice and service evaluation are not research. See the HRA's decision tool for do I need NHS REC review?

If you will be doing research under this definition, 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 uses. The HRA provides decisions based on this advice and issues approvals on behalf of the NHS for studies that are accessing data from NHS Trusts or GP practices.

More information: HRA Approval - Health Research Authority.

Examples of activities that could be research (and require approval): pre-market

The development of data-driven technologies (pre-market entry) would very likely be deemed research from an HRA perspective. For example, activities that could be considered research include:

- generating evidence to demonstrate that a data-driven technology, idea design or concept is workable
- testing, training or validating a technology in a live health environment (including clinical investigations)
- deploying a technology that is already on the market in a new setting (for example, moving from a hospital to a care home) or with a new population who are not represented in the data used in training or validating the technology

Examples of activities that could be research (and require approval): post-market

Some activities at the post-market stage may also be considered research. This includes post-market surveillance if a technology is being used outside of its intended purpose, or within its intended purpose but involving a change to standard care.

Important note: the definition of research used here to determine whether approval is required is narrower than the definition of research used by the ICO used in a data protection legislation context. However, the 2 definitions of research are not in conflict as they relate to your regulatory obligations.

Determining whether you are doing research as defined by the ICO is important to enable you to determine whether the research provisions that can be found in the UK GDPR and the DPA 2018 apply in any specific case. These provisions are aimed at helping you do your research more easily when appropriate safeguards are put in place in accordance with an appropriate legal basis.

Therefore, you should also check whether your activities pre- and post-market are research and, if so, what this means for your data protection obligations and your choice of UK GDPR legal basis. From an ICO perspective, for example, the development of a technology and the post-market surveillance of how that technology is performing when deployed will be seen as the development of a commercial product, using a lawful basis such as legitimate interests, rather than research.

For more information, see the ICO's guidance on research provisions, which gives advice on the application of data protection in this context.

Do you need research approval?

Read Is My Study Research and Do I need NHS Ethics approval 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 Confidentiality Advisory Group, in addition to REC approval.

Read: HRA approval and the Confidential Advisory Group

What approvals do I need?

If you plan to use data from NHS organisations for a research activity, you will 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 when it is from NHS patients or staff and will be provided by an NHS organisation; alternatively, if NHS resources/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 the 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. Read 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

How to comply with the UK GDPR as a developer

Step 6: Medical device clinical investigation approvals

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

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 need to apply also to the CAG (further guidance on how to do this can be found here).

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 the 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.

How to comply with the UK GDPR as a developer

Step 7: Follow the Caldicott Principles

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

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 may be sears 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.

How to comply with the UK GDPR as a developer

Step 8: Getting data from data providers

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

There are organisations that originally collected the data (for example, NHS Trusts, Universities). The original purpose of the collection may have been to provide clinical care, or to carry out studies including research activities. These organisations will already have made sure that the original collection of health data was lawful and fair. This would include ensuring appropriate lawful bases and compliant processing under UK GDPR.

Access to data is subject to the data provider's approval process. Different organisations may have different approval processes. You will need to contact them for advice on how to access their data and any contract that they require be agreed before you can access the data.

When you apply to get data from an NHS service provider who acts as an intermediary (such as NHS Digital), a research database, or a Trusted Research Environment/Secure Data Environment (both terms referring to a controlled digital environment used to store or analyse sensitive data securely), you should also check what requirements you must meet. This could include requiring you to first obtain researcher accreditation according to procedures they set out.

Carrying out these processes is separate from any research approvals you need to obtain. Therefore, you should include the additional time needed for this final stage in the calculation of your overall project timelines.

Get more information from:

- the Clinical Practice Research Datalink (CPRD)
- NHS England (NHSE) and its Data Access Request Service (DARS) with the Advisory Group for Data acting in an advisory role to NHSE, and
- the UK Health Security Agency (UKHSA)

Important note: when you want to 'repurpose' data collected for one purpose for a new purpose, UK GDPR requires you to have a new lawful basis in place before you engage in your so-called 'secondary processing'. However, if the new purpose is research as defined under data protection law, there are research exemptions that may be available to you. These include an exemption that means no new lawful basis is required in certain circumstances.

Therefore, it is important that you check if your purpose for using pre-collected data is research as defined by the ICO. If it is not research (which might be the case in some types of technology development activities), research exemptions would not be available and you will need to make sure you have a new lawful basis in advance of starting your secondary processing. Otherwise, if you want to use data for a new purpose that you did not originally anticipate when you collected the data, you can

only go ahead if the new purpose is compatible with the original purpose. Information on how to assess compatibility can be found in the ICO's guide on lawful basis for processing. However, it is not applicable if you are using data collected **by another organisation**. The law does not allow you to rely on compatibility with the original organisation's purpose, which means you will need to identify your own lawful basis to process the data.

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, to ensure your new processing is fair and lawful. You also need to make sure that you update your privacy information to ensure that your processing is still transparent.

Get more information:

Read about purpose limitation in the ICO's guide to the GDPR, and the ICO's guidance for research provisions within the UK GDPR.

