Developers guidance

Regulations for non-medical devices

Contents

Category

Technology idea

Technology idea

Creating a value proposition for digital technology in health and social care

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- United Kingdom

From:

- National Institute for Health and Care Excellence (NICE)

Last reviewed: 11 October 2024

If you want your digital technology to be placed on the UK health and social care market, you'll need to create a value proposition.

A value proposition is key to digital technology adoption

The National Institute for Health and Care Excellence (NICE) advises you to create a clear, purposeful value proposition for your technology in health and social care. It is one of the key first steps in the development process.

Deciding on a realistic value proposition and then proving your claim through evidence generation is fundamental to getting your technology adopted.

If your value proposition is limited or not backed up by evidence, it's highly unlikely your technology will be relevant and useful for the health and social care system in the UK.

The value proposition and why you need it

The value proposition is a statement of the value your technology could bring to the UK health and social care system. It usually includes information on:

- what your technology is intended to do
- who it is for
- how it works and
- why patients, health and care services might benefit from it

Below are the key elements of a value proposition.

Key element 1: identifying how your digital technology compares

Potential adopters will compare your technology's value with established clinical practice in health and social care, including the NHS. So, it is important that you identify what happens in current routine practice, and what value your technology brings relative to it.

The value your technology could bring generally falls under 2 categories:

- improving patient outcomes and
- reducing the use of health and care system resources

Key element 2: proving your digital technology is feasible

A key element of your value proposition is feasibility, and whether it is possible to generate evidence to support it. Collecting robust evidence to support your value proposition will take time and resources.

Example of a value proposition for a diagnostic technology:

'this technology improves patient outcomes and reduces unnecessary follow-up procedures by reducing the number of false positives compared with the current standard of care'.

Here's how to create and evidence your value proposition:

Step 1: Know your digital technology's intended use

Write your intended purpose statement. The value proposition is linked to your technology's intended use. This determines its qualification as a medical device and MHRA classification.

Step 2: Follow best-practice guidance and plan ahead

Use the resources below to help you write a value proposition:

NHSx guide to good practice for digital and data-driven health technologies

NHSx AI regulation guide: considerations when developing AI products

Think about using NICE's Office for Market Access service to help you understand your value proposition.

Test your ideas with users, such as NHS healthcare professionals and patients. This will help you develop a clear and relevant value proposition. It will also help you to identify

barriers to adoption of your technology. For more information, see researching user needs.

Step 3: Develop an evidence-generation strategy

Think about the order in which you want to collect evidence. You could start with near-term value and plan for longer-term data collection.

Follow guidance on how to generate evidence for your value proposition in NICE's evidence standards framework for digital health technologies and NICE's real-world evidence framework.

Also think about using NICE Advice Service to help you develop an evidence-generation strategy. This will support a NICE evaluation of your digital technology and market access.

See planning for evidence generation for more information.

Technology idea

Planning for evidence generation

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- Great Britain (England, Scotland, Wales)

From:

- National Institute for Health and Care Excellence (NICE)

Last reviewed: 03 November 2023

Last updated: 06 November 2023

Plan for evidence generation that proves your digital technology is safe, and clinically and cost effective.

Evidence generation to support your digital technology

As early on as possible, you should think about what evidence you will need to prove to assessors that your technology is useful.

Evidence is information on which a decision or guidance is based. You can gather evidence from a range of sources, usually through studies and research. This could include randomised controlled trials or observational studies.

Well-planned and implemented evidence generation will help you smoothly navigate regulations and commercial processes. Make sure you do this throughout the technology's lifecycle.

Plan to get the most out of evidence generation

You should plan to generate evidence that supports and is consistent with the intended purpose statement and value proposition of your digital technology.

You will need evidence to prove compliance with medical device regulations. You will also need evidence to prove to commissioners and health technology assessors (such as NICE) that your technology would be useful and worth adopting.

Planning makes sure you get the most out of your evidence generation and avoids duplication of effort.

For example, some regulators and commissioners may have the same evidence requirements. Or 1 piece of evidence may answer more than 1 question. You may be able to demonstrate safe use with users while capturing time savings in the same study. This could support 2 aspects of your value proposition.

Lack of planning could result in:

- disorganised or unfeasible evidence generation plans
- generating evidence of limited applicability to the UK health and social care system

This could:

- delay market access
- result in your technology no longer being financially viable to develop
- limit interest among adopters to buy the technology

Also think about how evidence-generation activities will change throughout the technology's lifecycle.

For example, to secure compliance before placing your technology on the health and social care market, it is key to have evidence that meets regulatory requirements for:

- safety
- performance
- usability
- interpretability, and
- interoperability

This also means planning to generate evidence on the most recent version of your digital technology.

How to plan for evidence generation

Identify all the specific evidence requirements from regulators, commissioners and health technology assessors. Plan how and when you need to answer these questions, and how much detail will be needed. You should also build in time to determine the most suitable study designs for evaluating your digital technology.

Remember you might need approvals for some steps of your evidence generation. This is particularly the case if you are doing research, including qualitative research. For example, you may need approval to do a clinical investigation of your medical device. This would be to meet clinical performance requirements.

For health technology assessors and commissioners, generate evidence in line with evidence standards and methods guides from NICE:

- NICE's health technology evaluations manual
- NICE's evidence standards framework for digital health technologies
- NICE's real-world evidence framework

Think about using NICE Advice. You'll gain expert feedback and actionable advice on your evidence generation plans, helping to demonstrate the impact of your product to NHS decision makers.

Review the Digital Technology Assessment Criteria tool. Adopters use this to determine whether evidence is sufficient to consider buying a technology.

Think about the resource requirements for each study including:

- funding sources
- time requirements
- collaborative partners

The MHRA's AI-Airlock will provide a regulator-monitored virtual area for developers to generate robust evidence for their advanced technologies. This will be launched in April 2024.

Technology idea

Avoiding algorithmic bias: data quality considerations for training and testing

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- Great Britain (England, Scotland, Wales)

From:

- AI and Digital Regulations Service

Last reviewed: 03 November 2023

Last updated: 06 November 2023

Successful digital technologies in health and social care are trained on high-quality machine learning datasets. To build healthcare technologies that adopters will buy, prioritise data quality.

Data quality for healthcare technologies

Think about data quality when developing plans for algorithm training, testing and validation. Also think about its appropriate generalisability to the UK market.

Generalisability means the degree to which you can apply research findings from a sample study to the whole population.

When adopters are reviewing your healthcare technology, they will consider many factors. These are related to the quality of the data used to train, test and validate your algorithms.

The data you use should be:

- representative of your target population in health and social care
- representative of the intended use of your healthcare technology
- technically high-quality (for example, the quality of images used to train an imaging technology)

If you train your algorithm on data that does not meet these requirements, it will not perform well.

Showing adopters that you have used high-quality data will build their trust and confidence in your healthcare technology. This makes it more likely that adopters will buy your technology.

Thinking about this early in the development process makes it less likely you will need to redo any steps related to algorithm development. This will save you time.

Data quality factors

Key data quality factors include:

Relevance of training and validation datasets:

- Do they contain information on the relevant patient population?
- Do they contain enough information on different population groups of interest?
- Do the data sources have information on relevant exposures, outcomes and other covariates?
- Does the dataset cover the range of intended settings in which the technology will be deployed?
- Does it represent the full range of users or patients in the real-world setting? Have marginal cases been sufficiently represented?
- Are the results likely to generalise to routine clinical practice? For example, are they representative of the population who would use the technology (according to your intended use). Would the results be applicable to the health and care settings in which it would be deployed?

Quality of training and validation datasets:

- To what extent is data missing on key variables (exposures, outcomes and covariates)?
- How valid are the measurements for key variables?
- Are the key variables consistently recorded across patients and over time?
- Is there enough data?

External validation:

- Does the technology perform well in datasets or systems that were not used for algorithm development?

Other considerations:

- Does the technology introduce any ethical or equity issues?
- Does your data-labelling process involve quality management, including addressing ways in which AI bias could be inadvertently inserted into the dataset?

How to ensure data quality

It's important to ensure data quality throughout the lifecycle of your healthcare technology. You need to consider the quality of your data when:

- training datasets for model development
- testing datasets for model evaluation and parameter variation
- validating (internally and externally) datasets for meeting user needs
- updating your technology or expanding its intended use

Use these tips when training your algorithm:

- use different datasets for testing and validating your technology
- test the clinical performance of your digital technology in systems that were not used during algorithm development. This ensures you are validating your technology to determine how well it performs in datasets that were not used for algorithm development
- read STANDING Together's recommendations for diversity, inclusivity, and generalisability in artificial intelligence health technologies and health datasets
- read guidance from the ICO on the risks of bias and discrimination in a dataset
- use appropriate tools to support your data-quality management. These include technical tools that enable you to test for bias as well as governance mechanisms that provide auditable documentation, metadata templates and assurance. The tools you use will be specific to your intended use and target market. For example, CONSORT-AI and SPIRIT-AI provide reporting guidelines for clinical trial protocols and reports

Technology idea

Researching user needs

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- United Kingdom

From:

- National Institute for Health and Care Excellence (NICE)

Last reviewed: 11 October 2024

Knowing the user needs of your digital technology in the health and social care space is critical to your success. Researching and defining user needs is therefore an important first step in a user-research plan.

The importance of knowing what your users need from your digital technology

Knowing user needs will help you:

- determine if your digital technology is relevant and useful for the health and social care system
- develop a clear and relevant value proposition and identify any possible barriers to adoption of your digital technology

If you do not understand user needs, your digital technology is not likely to meet them, and so adoption of your technology will be unlikely.

Users are anyone who would use your digital technology. This includes patients and their families, carers, health and social care staff, or a combination of these. User needs are the needs that a user has of a service. That service must meet the needs of the user and provide them with the right outcome.

Research user needs: how to do it

User needs within health and social care systems are complex. There may be existing capacities or methods for solving the problem you are trying to solve, and any new digital technology could disrupt current systems. So it’s essential to understand people's entire experience around the technology or service you're building.

Follow guidance on researching user needs in:

- the Department of Health and Social Care's guide to good practice for digital and data-driven health technologies
- the Government Digital Service's manual on user research
- the NHS Digital service manual

Also think about your full user-research strategy. Users should be involved as much as possible throughout the technology’s lifecycle (conceptualisation, development, design and post-market review).

Technology idea

Complying with NHS Digital clinical risk management standards

This is required guidance

It is legally required and it is an essential activity.

From:

- NHS England

This Guide covers:

- England

If you want your digital technology to be adopted by the NHS, you need to meet safety standards set by NHS Digital.

The NHS Digital standards

NHS Digital has issued 2 clinical risk management standards:

- DCB0129, which applies to developers
- DCB0160, which applies to adopters

These standards require both developers and adopters to do a risk assessment on the digital technology.

As a developer, standard DCB0129 requires you to:

- create a clinical risk management system
- do clinical risk analysis

This is done to support the safe development of digital technology in health and social care.

If your digital technology cannot meet standard DCB0129, you will not be able to place it on the market. Adopters will not be able to use your technology in the NHS.

How to meet the NHS Digital standard DCB0129

As a developer, you must:

- do a clinical risk assessment
- provide evidence of effective risk management
- present your findings to the adopter

Use the relevant standard DCB0129 Clinical Risk Management: its application in the manufacture of health IT systems.

This standard requires you to detail and evidence that a clinical risk management system is in place. This includes:

- clinical risk management governance arrangements

- clinical risk management activities
- clinical safety competence and training

You must start your clinical risk management process at the earliest stage of your development lifecycle and continue to assess and gather evidence throughout development.

It is important to note that risk management includes digital technology maintenance and decommissioning. So, also plan how to monitor and manage risk assessment after deployment.

Adopters will assess whether you have complied with DCB0129 before they can deploy and use your technology.

Adopters also want to know whether you have followed good-practice principles. The Digital Technology Assessment Criteria (DTAC) establishes good practice in key areas of digital technology development, including clinical risk management. It forms the new national baseline criteria for digital technologies entering the NHS and social care.

Meeting DTAC criteria means your digital technology is meeting national baseline criteria.

You can use the NHS Digital document templates to help you complete your clinical risk management requirements. It is important that staff have the appropriate knowledge, experience and competencies to do the risk management tasks assigned to them.

Risk management of medical devices

If you are developing a medical device, you will also need to comply with the International Organization for Standardization's ISO 14971:2019 medical devices - application of risk management to medical devices.

Read more about risk management for medical devices in Meeting ISO 14971 risk management requirements for medical devices.

If you are planning to implement your medical device in a health IT system, then you must also comply with DCB0129.

Technology idea

Using the Digital Technology Assessment Criteria (DTAC)

This is best practice guidance

Although not legally required, it's an essential activity.

From:

- NHS England

This Guide covers:

- England

DTAC for health and social care

If you want your technology to be used in the NHS and social care, it needs to meet the standards set by the DTAC.

During procurement, adopters will review your completed DTAC to assess if your technology meets minimum baseline standards. If your technology meets the standards, adopters feel assured they are buying a safe and effective technology. They are then more likely to buy your technology.

Completing the DTAC

It's important to understand the assessment criteria and consider whether your healthcare technology meets the required standards. Make sure you are meeting the criteria during technology conceptualisation and throughout the technology's lifecycle.

The DTAC focuses on 5 core areas:

- clinical safety
- data protection
- technical assurance
- interoperability
- usability and accessibility

The DTAC brings together legal requirements and best practice in these areas. It overlaps with other legal requirements, such as conformity with medical device or data protection regulation.

For example, the DTAC requires you to:

- provide proof you have obtained a UKCA mark (or recognised equivalent) and details of your risk management system
- follow related guidance on data protection and demonstrating clinical safety
- follow related guidance on interoperability, usability and accessibility in the GOV.UK guide to good practice for digital and data-driven health technologies

Using the DTAC

To meet the DTAC standards you need to:

- review the Digital Technology Assessment Criteria for health and social care
- consider whether your healthcare technology would meet the minimum standards, including the adopter risk-assessment criteria
- plan how to build the required standards into the design of your technology
- document all your processes to produce evidence demonstrating your technology meets the required standards

If you have questions about the DTAC, contact england.dtac@nhs.net

Using the NHS digital service manual

Use these components in the NHS digital service manual to help you develop your technology and check you're working to best practice from the start:

- the NHS service standard helps you meet the GOV.UK service standard for technologies or services in health and care. Commissioned services are expected to meet the service standard and may be assessed against it, as well as the DTAC criteria of usability and accessibility. The about technology section gives more detail about common tools you should consider using. These include the NHS login to authenticate identity, and the Personal Demographics Service to access and manage patient data
- the design system helps you meet usability and accessibility requirements. This can save the NHS money by reusing existing code. It also provides trusted NHS branding and easier user journeys between systems and services

Note that technology and software may be considered a medical device depending on its intended purpose. See writing an intended purpose statement for more information.

Technology idea

Understanding technical standards for digital technology in health and social care

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- Great Britain (England, Scotland, Wales)

From:

- AI and Digital Regulations Service

Last reviewed: 25 August 2022

To increase trust and confidence in your digital technology, you should show compliance with technical standards.

The importance of technical standards

Meeting technical standards is an efficient way to demonstrate the reliability and quality of a digital technology. This increases trust and confidence with regulators and adopters.

A standard is a document that provides uniform rules or guidelines for:

- specific technologies or services
- production methods
- management systems processes

Your organisation can produce these formal documents for internal guidance. However, specific standards produced by recognised standards organisations can provide a common set of rules and guidelines across a sector, nationally and internationally.

Standards are developed by panels of experts who work together to find an agreed set of rules or guidelines. Some standards are referenced against specific regulations, such as medical device regulations. These are referred to as designated standards.

Standards are recognised by a:

- prefix that identifies the geographical region it aligns with
- title
- unique number, and
- publication year

It is important to make sure you are following the most recent version of a standard and that it is recognised in the region you operate. For example, the term ISO indicates that the standard has been assessed and recognised by the global harmonisation body International Organization for Standardization.

Examples of these include:

- ISO 13485
- ISO 14971

Designated standards

Following digital technology technical standards is best practice and all standards are voluntary. However, a 'designated' standard is recognised by government in part or in full. Designated standards enable developers and service providers to claim 'presumption of conformity'. Combined with associated evidence, this shows you have met the related legal requirements. Showing compliance with designated standards will help you access the market.

You can meet the legal requirements without following specific standards. However, you would need to provide evidence that your alternative method is robust, appropriate, and not inferior to the standardised approach. And it may be challenging to find an approved body willing to assess a technology against a non-typical set of criteria.

Following general standards

Think about your organisational goals. There are general standards that may be applicable to your company's ethos and vision. Demonstrating compliance with these standards increases customers' trust in your organisation. For example:

- quality management
- sustainability
- social responsibility

Following technical standards

Identify the technical standards you wish to comply with at an early stage. This helps you manage your risks and development processes as well as operation of the technology or service. It also allows you to interact with regulators and supporting services early on, to plan the most efficient and safe access to market.

You also need to select standards that are specific to the technology or service you are developing. This could be standards for:

- medical devices
- product quality
- customer satisfaction

- meeting state of the art

Speak to your industry association or national standards organisations to help you identify the most relevant standards. If you plan to develop for the international market, then it will be important to consider international standards. These are developed by organisations such as ISO, IEC, IEEE or other national organisations such as AAMI (US). Usually, these standards have been aligned with national standards.

It is useful to research the standards your competitors are using and that customers prefer, and the reasons why.

Also consider the standards that are used throughout the supply chain to make sure your technology or service is fully compatible for the health sector.

Purchasing a standard

Standards are not open access, so you will need to buy them. The cost should be factored into your budgeting. The cost of not following recognised standards can be greater because of:

- inefficient development
- poor risk management
- poor evidence gathering
- not demonstrating compliance with regulation

Not using the standards can put you at a competitive disadvantage and result in lack of confidence or trust of customers.

Applying a standard

It is worth purchasing accompanying guidance documents to help you apply the selected standards. Engaging with innovation services, our team at the AI and Digital Regulations Service and the regulators will also help you because they can offer expertise and guidance. If a skills gap is identified in your organisation, you can employ consultants to advise on standards.

Changing technical standards

Standards are reviewed every few years and updated versions are published, with amendments or appendices. This is particularly the case in AI because the technology and its use are continually developing. You will see which version is the most recent because it will include the year of the update.

This information is not intended to replace formal statutory guidance regarding legal requirements. For an authoritative view of what regulations require beyond this digest, please see the relevant gov.uk web pages pertaining to the MHRA.

Technology idea

Implementing a quality management system for your technology

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- Great Britain (England, Scotland, Wales)

From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

Although not legally required for non-medical devices, implementing a quality management system (QMS) is best practice and essential to placing your technology on the market.

What is a quality management system?

A QMS outlines processes that minimise the risks associated with the production, deployment and surveillance of technologies. A QMS provides structure for key company processes. These internal processes and policies ensure:

- robust documentation management
- risk assessment
- tracking of key decisions and
- clear routes for sign off

Depending on scope, a QMS will help you with activities that may include:

- design and development
- evidence generation
- post market surveillance

Your QMS should evolve in line with company aspirations and throughout the lifecycle of the technology.

Management systems can take significant time and personnel to set up, certify and operate. So, make sure you set up your QMS during technology conceptualisation and wider strategic planning.

To learn more, please review our guidance on setting up a QMS for medical devices. Although this guidance is tailored to medical devices, it gives a complete overview of what you need to do to meet best practice principles.

Category

Technology development

Technology development

Designing clinical studies and choosing evaluation methods for your digital technology

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- United Kingdom

From:

- National Institute for Health and Care Excellence (NICE)

Last reviewed: 11 October 2024

You need to regularly evaluate your digital technology to show adopters and assessors it's effective and safe.

Supporting your digital technology through evidence

Adopters, health technology assessors and regulators need evidence that shows your technology:

- works in practice
- is clinically effective
- is cost effective, and
- is safe

Spend time thinking about your study designs and evaluation methods. This will help produce the best possible evidence to support your digital technology.

Not planning upfront may result in inappropriate evidence generation. Or, it could result in missed opportunities to generate the most relevant evidence.

Gathering relevant evidence at each stage of the technology's lifecycle

You need to evaluate your digital technology at various stages throughout its lifecycle. The type of evaluation will vary at different stages. Thinking about this early on helps you produce the most relevant evidence at each stage. For example:

- during technology conceptualisation, you may do proof-of-concept evaluation studies
- during technology development, you may do a validation study and a clinical investigation
- during post-market stages, you may do a real-world evidence study. This will show how well your technology works in practice. Follow guidance on how to generate trusted real-world evidence in NICE's real-world evidence framework.

Steps to designing clinical studies and choosing evaluation methods

Step 1: Level of evidence

Determine the level of evidence required by adopters, health technology assessors and regulators. For more information, see:

- submitting evidence to get a UKCA mark
- generating evidence for health technology assessment
- generating evidence for adopters

Step 2: Designing your evaluation

Design your evaluation and choose your evaluation methods. See information from the Office for Health Improvement and Disparities on how to design your evaluation and choose your evaluation methods.

Step 3: Feasibility of evaluation

Think about feasibility. You may need to weigh:

- the effectiveness of data collection methods, with
- the time and resources needed to do them

Try to get the most out of your studies by answering different questions at once, if possible. For example, capture cost-effectiveness evidence at the same time as safety and performance data.

Technology development

Generating evidence for NHS adopters of digital technology

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- United Kingdom

From:

- National Institute for Health and Care Excellence (NICE)

Last reviewed: 11 October 2024

If you want the NHS to adopt your digital technology, you will need to generate evidence that supports your technology's value proposition.

Evidence to support the value proposition of your digital technology

Adopters in health and social care will want to see evidence that supports your technology's value proposition. Generating the appropriate evidence will increase the likelihood that the NHS will adopt your digital technology.

If you do not generate the appropriate evidence, it's unlikely that adopters will buy your technology.

How to generate evidence for your digital technology

Use NICE's evidence standards framework for digital health technologies. This will help you determine the minimum range of evidence you will need to provide to adopters.

In general, you will need to provide evidence of:

- your digital technology's value proposition and whether this is relevant to each adopter's specific circumstances
- clinical and cost effectiveness (similarly to evidence for NICE), including overall economic impact on the health and care system
- your technology's safety
- the acceptability of your digital technology with users and clinicians
- compliance with relevant regulations

Some of this evidence will be identical to the evidence required to get a UKCA mark. Adopters will want to know whether your digital technology has a clear and feasible implementation strategy. They also want to know whether its adoption would be scalable and sustainable.

Consider using NICE's advice services:

Our NICE Advice service helps you optimise your approach at any point in product innovation and development, especially in the early stages. We can support you to:

- understand your product route to market
- review your development and evidence generation plans
- identify what matters most to patients, as well as the health and care system
- engage with the system during product development to support adoption and use.

Technology development

Qualitative research: collecting data on your digital technology

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- United Kingdom

From:

- National Institute for Health and Care Excellence (NICE)

Last reviewed: 11 October 2024

Qualitative research will give you a much richer understanding of how a user interacts with your digital technology.

Benefits of qualitative research

Collecting qualitative data is an important part of doing user research.

Qualitative data helps you:

- understand how health and social care staff would interact with data produced by your technology
- identify any barriers to using the data for clinical decision-making

Users may have a lack of trust in technology. This is a common barrier to the successful implementation of digital technology. For example, patients and staff may not understand AI decision-making. That's why qualitative data on user acceptance is particularly important for AI technologies.

Qualitative research definition

Qualitative research involves collecting and analysing non-numerical subjective data. You do this by using methods like interviews and field studies. This helps you understand a user's attitudes, thoughts and beliefs.

Qualitative research can give you a richer explanation of what is happening when someone uses your technology.

Difference between qualitative and quantitative research

Quantitative research can describe:

- patterns of disengagement with an app
- what demographic factors predict disengagement

Qualitative research can describe **why** a user stopped using the app.

How to do qualitative research

Determine if qualitative research would be useful. For example, you should do qualitative research if you need an in-depth understanding of a user's thoughts and experiences.

Compare different qualitative study designs and choose an appropriate method. See guidance on qualitative studies from the Office for Health Improvement and Disparities.

Analyse the data. The most common method is thematic analysis. See guidance on how to analyse qualitative data from the Office for Health Improvement and Disparities.

Category

Placing a technology on the UK market

Placing a technology on the UK market

Regulated activities: check if you need to register with the Care Quality Commission (CQC)

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Care Quality Commission (CQC)

Last reviewed: 10 October 2024

If you are providing, or you intend to provide, health or adult social care activities in England, you may be legally required to register with the Care Quality Commission under the Health and Social Care Act 2008.

The Care Quality Commission

The Care Quality Commission (CQC) is the independent regulator of health and adult social care in England.

It makes sure health and social care services provide people with safe, effective, compassionate and high-quality care and encourages services to improve.

If you provide an activity that is in the scope of registration, you are required by law to register with CQC.

Check to see if you are providing an activity in scope. You'll only need to register with CQC if you do.

Regulated activities

The regulated activities are:

- Personal care
- Accommodation for persons who require nursing or personal care
- Accommodation for persons who require treatment for substance misuse
- Treatment of disease, disorder or injury
- Assessment or medical treatment for people detained under the Mental Health Act 1983
- Surgical procedures
- Diagnostic and screening procedures
- Management of supply of blood and blood-derived products
- Transport services, triage and medical advice provided remotely
- Maternity and midwifery services
- Termination of pregnancies
- Services in slimming clinics
- Nursing care

- Family planning services

For a more detailed explanation of who may need to register and a description of each regulated activity, see CQC's scope of registration.

When artificial intelligence (AI) or digital technologies form part of a regulated activity

If you use AI-driven technologies as part of delivering a service, you need to check if the adoption and use of the technology constitutes a regulated activity. If you determine that it is a regulated activity, **and you are not already registered with CQC to provide it**, you will be 'carrying on' the regulated activity and will therefore need to register.

It is the use of this technology that may be a regulated activity, rather than the supply of the technology.

If you are supplying AI, which another care provider uses to provide a regulated activity, you do not need to register, but they may need to.

Example:

Need to register: your company makes a diagnosis using AI and sends the results back to the referrer who does not double check your diagnosis.

You do not need to register: your company supplies AI to an NHS or other healthcare provider. That provider, and its clinical teams, use the AI-driven technologies to make a diagnosis.

CQC registration

To register with CQC, you need to show that you meet requirements. You must also show you will provide and manage services that are safe, effective, caring, responsive to people's needs and well led.

Submit your application to CQC

If you need to register, submit your application online to CQC.

Register as a new provider on CQC's website

Category

Technology in use

Technology in use

Understanding how the Care Quality Commission (CQC) regulates health and social care services

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Care Quality Commission (CQC)

Last reviewed: 10 October 2024

The Care Quality Commission (CQC) is the independent regulator of health and adult social care in England. It makes sure health and social care services provide people with safe, effective, compassionate and high-quality care. CQC also encourages care services to improve.

If you provide a regulated health or social care activity in England, you are legally required to register with CQC. This page will help you to understand:

- which regulations you must meet
- when they may apply

CQC regulates health and adult social care services in England only. Check local regulations for delivering health and social care services in the devolved administrations, for example:

- in Wales, the Care Inspectorate Wales
- in Scotland, the Care Inspectorate
- in Northern Ireland, the Regulation and Quality Improvement Authority

When a digital technology is used to provide regulated health and social care services, developers and adopters need to know what regulations apply.

CQC registration

If you provide a regulated activity, you are legally required to register with CQC. Please read the 'Check if you need to register with the CQC' guide for further information on when and how to register.

When applying for CQC registration, you must show that you will be able to meet the regulations in the Health and Social Care Act. Once registered, you must show that you will continue to meet them.

CQC's approach

CQC regulates services to make sure they meet:

- the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (including the fundamental standards)
- the Care Quality Commission Registration Regulations 2009

This involves using data and on-site inspection activity to assess the quality of care. CQC publishes its findings, including quality ratings.

CQC uses different methods and sources of evidence to assess the quality of care, depending on the type of service provided. This is to understand if services are safe, effective, caring, responsive and well-led.

CQC inspection teams might want to:

- check technologies are safely and effectively deployed in the care pathway (completing a data protection impact assessment before deployment may help demonstrate how data protection risks were considered and mitigated)
- see evidence that relevant staff have been appropriately trained in using any new technologies
- see that processes are in place for appropriate reporting of any issues or incidents relating to new technologies

When do the regulations apply?

If the use of digital technology constitutes an activity regulated by CQC, and you are not already registered to provide that activity, you will need to register and demonstrate that you can meet the fundamental standards.

Check to see if you provide an activity in scope of registration. You'll only need to register with CQC if you do.

CQC's assessment framework

CQC is developing a new single assessment framework to assess whether services meet regulations. It will do this by asking 5 key questions: whether services are safe, effective, caring, responsive and well led.

Quality statements under each key question describe what good care looks like. The assessment framework sets out the 6 categories for the type of evidence CQC collects. This will depend on the service type (for example, a GP practice) and the level at which CQC is assessing (for example, at registration).

For more information, see:

- CQC's key questions and quality statements
- CQC's new single assessment framework

Guidance on meeting CQC regulations

See CQC's guidance for providers on meeting the regulations.

For more information on the inspection process when CQC makes an on-site visit, see CQC's what we do on an inspection.

Technology in use

Ongoing research and service evaluation of your digital technology

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- United Kingdom

From:

- National Institute for Health and Care Excellence (NICE)

Last reviewed: 11 October 2024

After placing your digital technology on the health and social care market, you may need to produce more evidence to prove its cost and clinical effectiveness. You should plan for this upfront to prevent the delay or further development of your digital technology.

Providing ongoing evidence to support your digital technology

NICE and adopters need to determine the cost and clinical effectiveness of your technology. They do this by looking at the evidence you have generated. This is an essential part of placing your digital technology on the market.

Although preferable, sometimes you may not be able to generate evidence early on. If this is the case, you will need to produce further evidence after your digital technology has launched.

Further research and service evaluation often takes place after you've placed your technology on the market. For example, you may need to do this after you have obtained your UKCA mark.

Planning for research and evidence generation

It is important to plan ahead to produce the best possible evidence to support your digital technology.

Not planning upfront may result in missed opportunities to generate the evidence needed. This could delay or limit further deployment of your technology.

Step 1: knowing the level of evidence required

Determine the appropriate level of evidence you need to generate for NICE or adopters. Determine the appropriate study designs to generate this evidence.

Step 2: find out if you need research approvals

Determine whether you need approval from the Health Research Authority (HRA) for further research. Service evaluations and audits are not considered research and do not need specific research approval.

Difference between research and service evaluation

There is an important distinction between research and service evaluation.

Service evaluation:

- involves the routine monitoring of data to review the technology's performance in the service it is deployed in
- is essential for adopters to determine the technology's impact on the performance and safety of their service
- does not usually provide appropriate evidence to assess the clinical and cost effectiveness of your technology in practice. So, you are likely to need to do further research in the post-market stage

Research:

- provides evidence to prove the clinical and cost effectiveness of your digital technology
- will require approval from the HRA
- is essential for placing your digital technology on the market

Category

Updating your technology

Updating your technology

Improving or updating digital technologies after deployment

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- Great Britain (England, Scotland, Wales)

From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

Last reviewed: 25 August 2022

When updating digital technologies that are already on the UK health and social care market, you will need to consider if previous evaluations (for example, health economic modelling) are impacted by the change and whether any standards used are still being met. Additionally, new functionality and claims may result in your technology becoming a medical device and should be reviewed ahead of making an update.

To learn more, please review our guidance on Improving or updating digital technologies after deployment. Although this guidance is tailored to medical devices, it gives a complete overview of what you need to do to meet best practice principles.

This information is not intended to replace formal statutory guidance regarding legal requirements. For an authoritative view of what regulations require beyond this digest, please see the relevant gov.uk web pages pertaining to the MHRA.

Category

Regulations that govern the use of data

Regulations that govern the use of data

Data regulations for digital technologies in health and social care: a guide

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

Reviewed by: Health and Care IG Panel

Please note: a longer and more technical version of this guidance is available on the website of the Health Research Authority (HRA): Legal requirements for using health and care data in data-driven technologies Health Research Authority (hra.nhs.uk). Refer to this longer guidance and its glossary for an in-depth analysis of your legal obligations and the laws in this area (including reference to primary legal definitions). You can also find other important health and care research guidance on the HRA's website.

For comprehensive general guidance on UK data protection law, see the ICO's website.

For guidance on information governance (IG) in the health and care sector in general, see the NHS Transformation Directorate IG Portal. This brings together national IG guidance to help those working in the health and care sector understand how to use information appropriately to support care. It includes guidance focusing on the IG implications of using AI in health and care settings, which you should refer to because it helps support the lawful and safe use of data for AI innovations.

Revolutionising health and social care with digital technologies

Digital technologies have enormous potential to improve health and social care. For example:

- sensory technology could track patients at home, assisting independent living
- apps could help patients talk to their clinicians and better manage their health
- data-driven digital tools could help clinicians better diagnose and treat conditions

It is data that powers these innovations, but data usage must comply with laws and regulations. The good news is that the laws and regulations governing the use of health and care data aim to make data sharing possible for a range of purposes, including the development of data-driven technologies. Therefore, understanding these legal and regulatory frameworks is key to realising the potential of digital technologies.

This guide will help you learn:

- what laws apply to using health and social care data at each stage of your technology's lifecycle
- how to implement a data protection 'by design and by default' approach
- how and when to undertake a data protection impact assessment (DPIA), and how it will benefit you and the patients/service users you serve

- when you need to get research approval from
  - the Health Research Authority (HRA)
  - Health and Care Research Wales (HCRW)
  - a Research Ethics Committee (REC), and/or the Confidentiality Advisory Group (CAG), and
  - when you need to follow guidance set out by the Medicines and Healthcare products Regulatory Agency (MHRA)

Regulations that govern the use of data

Understanding types of health and care data

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

Reviewed by: Health and Care IG Panel

Two types of health and care data can be distinguished to help you determine when the relevant legal and regulatory frameworks apply:

1. Data that relates to identified or identifiable individuals. **Confidential patient and service-user information** includes information that identifies or could be used to identify the individual (such as name and address), relating to, or in connection with, an identified or identifiable individual's past or present use of services (NHS or adult social care). This broad definition is in recognition of the importance of maintaining trust in health and care services, so that all individuals can be reassured in fully engaging with these services that their confidential information will only be used in ways that they reasonably expect.
2. Data that does not or no longer relates to identified or identifiable individuals **(anonymous data)**, such that the process of rendering the data anonymous means that the laws that apply to the modified data no longer apply to those receiving it.

Important note: data can be rendered anonymous in different ways. One way is by applying a machine-learning model to a real-world dataset. For example, real-world derived synthetic data can be generated by creating average results from a large set of data. This type of synthetic data can be distinguished from synthetic data that is totally made up with no relationship to anyone living or dead (hereafter called 'artificial data').

When data is generated to statistically mimic real-world data that it replaces, an assessment should be carried out regarding the likelihood of individuals being re-identified from the synthesised data. If necessary, additional safeguards may be needed to make sure that any re-identification risks (or other privacy risks) are sufficiently remote so that it may be considered anonymous.

Get more information:

ICO guidance on anonymisation, pseudonymisation, and privacy enhancing technology

Regulations that govern the use of data

Understanding laws that regulate the use of health and care data

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

Reviewed by: Health and Care IG Panel

In the UK, the **UK General Data Protection Regulation (UK GDPR)**, supplemented by the **Data Protection Act 2018 (DPA 2018)**, governs the processing of 'personal data' (a defined legal term). The UK GDPR mirrors the provisions of the EU General Data Protection Regulation that came into effect in 2018, before the UK left the EU. The UK GDPR and DPA 2018 only apply to the processing of data that **relates to identifiable living people.**

The common law duty of confidentiality governs the disclosure of confidential patient and service-user information. It applies to information that can **identify either living or deceased people.**

In this guide, we use the terms as they apply under each framework. When we refer to:

- data protection legislation, we will use 'personal data'
- the common law duty of confidentiality, we will use 'confidential patient and service-user information'

These laws exist to make sure you use people's data in a legal, fair and transparent way, and that data is only processed or disclosed in ways that a person would reasonably expect. 'Processing' under article 4 of UK GDPR means any operation or set of operations that is performed on personal data such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction. These laws also aim to make data sharing possible for a range of purposes, including research and the development of AI and digital technologies.

Regulations that govern the use of data

Using data during your digital technology lifecycle

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

Reviewed by: Health and Care IG Panel

At each stage of your technology's lifecycle, you will need to use data.

Proof-of-concept (pre-development)
This involves generating evidence to show that a technology idea, design or concept is workable.

Technology development
This includes the following stages:

- **Testing in the health or care environment** (technology conceptualisation)
  Before you can deploy your technology in clinical care, you must show it is safe and effective to use. You might need to test this in a live health or care environment
- **Direct care** (technology rollout once placed on market) (deployment)
  Direct care (also known as individual care) is any clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. More guidance relating to the use of data for direct care and the direct-care concept can be found on the NHS Transformation Directorate IG Portal. To be part of the direct care team, you must have a legitimate relationship with the patient or service user, such that the individual would reasonably expect you to have access to their records to provide them with individual care
- **Service evaluation and post-market surveillance** (post-rollout)
  Once you have rolled out your technology, you will have to monitor it for safety and efficacy

Regulations that govern the use of data

Proof-of-concept: using anonymous or artificial health data

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

Proof-of-concept: using anonymous or artificial health data

Reviewed by: Health and Care IG Panel

Often, developers will use anonymous or artificial data (that does not, or no longer, relates to identified or identifiable individuals) during their proof-of-concept stage. The data you choose should still be appropriate to the context of the technology you are investigating.

Benefits of using anonymous or artificial data during proof-of-concept:

- it can speed up your technology's route to market, because you will not need to wait for consent or approvals
- the results of your proof-of-concept can justify why you need to use personal data at a later stage
- it reduces the risk/detriment to patients if a data breach occurs while you are developing your technology

Data minimisation

Designing your technology to minimise processing of personal data to what is needed is also a legal requirement under UK GDPR. Even if personal data can be justified as necessary, it must be minimised to only the amount of data needed to carry out the project purpose at that stage and no more. Data minimisation is also a requirement of the Caldicott Principles relating to confidential data in health and social care, which you must follow. For example, the Caldicott Principles state that the minimum data possible should be used and accessed strictly on a 'need to know' basis. For more information, see step 7 in complying with the UK GDPR.

When developing a digital technology, therefore, you need to consider the kind of data that is the best fit for each stage of development. This is to make sure you only use what is necessary and proportionate to achieving your purposes at each stage.

The UK GDPR also requires you to put in place technical and organisational measures to fulfil the data protection principles and safeguard individual rights. This approach is described under Article 25(1) and (2) as 'data protection by design and by default'. Your first consideration should be: what kind of data do I need for the development stage of my technology? At proof-of-concept stage, using artificial or anonymous data may be a better choice than using personal data or confidential patient/service-user data and will reduce your level of risk, as described below. Building data protection functionality such as access controls, audit trails, and appropriate privacy notices for the intended users is an effective way of meeting this data protection legal requirement.

Get more information: Data protection by design and default | ICO

How to process anonymous or artificial data

Usually, you do not need consent or approval to process data that has been rendered anonymous (including through synthesis), or artificial data. This is because, when a person cannot be identified from data, its use is not subject to the UK common law duty of confidentiality or data protection legislation.

Anonymous data

Data rendered anonymous data is no longer considered personal data. See the ICO's guidance on what is personal data?

Important note: Determining whether the data you wish to use is personal data or not is your responsibility and you should carry out your assessment helped by the latest guidance provided on the ICO website. You should check the ICO website from time to time as new guidance becomes available.

In this process of anonymising personal data, an organisation has modified data in order to share it with a third-party organisation, while also putting in place additional processes and other appropriate safeguards to prevent the use of means reasonably likely to identify the individual in the third-party's hands, and thus make sure it meets effective anonymisation requirements. A key benefit of this is that it reduces risk of a data breach of personal data, which could cause harm to patients and service users.

A lawful basis is required to anonymise personal data (see step 4 in complying with the UK GDPR: Have a lawful basis for processing health data). In particular, a lawful basis under the common law duty of confidentiality is required to share confidential patient and service-user information with someone who would then apply anonymisation processes to the data. If the person receiving the data is not part of the direct care team looking after the individual, there will be a disclosure of confidential information (albeit solely for the purposes of anonymising it) and a legal basis to lift the common law duty of confidentiality is required. This would likely apply to a technology developer. In such circumstances, you must obtain the prior explicit consent from the individual, unless there is another legal basis available to you, as described further below.

Important note: this type of consent (explicit consent from an individual to permit confidential information to be shared outside the team directly caring for them) is separate from UK GDPR consent. However, the rules on consent do not conflict. This is because they are about consent for different things under 2 different sets of regulations that were created to work together without tension. For more on this distinction, see the NHS Transformation Directorate's guidance on consent and confidential patient information and the HRA's guidance on consent in research.

Important note reminder: if you are reliant on using anonymous data to fall outside the law, you must make sure the data you want to use has been rendered anonymous, and you have evidence to demonstrate that it is no longer personal data, before using or disclosing it. Any onward transfer of (or remote access to) the data may change its status to be personal data again, depending on any additional information and means available to the onward recipient. Therefore, the effectiveness of your anonymisation strategy must be determined on a case-by-case basis, using the latest guidance provided on the ICO website.

A note on pseudonymisation

Pseudonymisation is a technique applied in circumstances when the link between individuals and the data that relates to them needs to be reduced but not removed entirely. It involves replacing information in a data set that directly identifies an individual. For example, it could involve replacing an NHS number, a name, or an address, with a unique number or code (a pseudonym). This has the effect that those receiving it cannot identify an individual directly from that data without access to additional information held separately and securely elsewhere (for example, the 'key' that would enable matching the pseudonym to the removed direct identifiers).

UK GDPR legislation applies to personal data. The UK GDPR considers that pseudonymisation is not an anonymisation technique. This is because, by itself, applying the technique does not render personal data anonymous in the hands of those receiving the information. More is required, such as putting in place a data-sharing contract and other appropriate safeguards to prevent reidentification by the recipient. The determining factor is whether or not the recipient can use the modified data (whether on its own, or in conjunction with other available data using reasonable means) to identify an individual.

If you are using pseudonymised data, make sure you understand your legal obligations described in how to process health data.

Get more information:

ICO guidance on anonymisation, pseudonymisation, and privacy enhancing technology

Regulations that govern the use of data

Using health data during technology development

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

Reviewed by: Health and Care IG Panel

You may need to use personal data during the development stage of the technology. This is because using synthetic data or anonymous data may not be appropriate for the clinical-environment validation of the performance and safety of your technology.

When using **personal data**, remember that you need to have a lawful basis for doing so under data protection legislation (within the UK GDPR). The disclosure of any **confidential patient and service-user information** to you as a developer (when you do not work as part of the direct care team) will also need to have a lawful basis under the UK common law duty of confidentiality. This avoids harm to patients or service users from improper use of data. Otherwise, you may risk prosecution, a fine or damage to reputation.

How to process health and care data

When processing personal data related to health and care provision, you need to follow the requirements of the:

- UK GDPR (if the individual is still living) and
- common law duty of confidentiality (for both living and deceased individuals)

Regulations that govern the use of data

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

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.

Regulations that govern the use of data

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.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

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

Regulations that govern the use of data

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.

Regulations that govern the use of data

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.

Regulations that govern the use of data

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.

Regulations that govern the use of data

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

Regulations that govern the use of data

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.

Regulations that govern the use of data

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.

Regulations that govern the use of data

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.

Regulations that govern the use of data

Common law duty of confidentiality

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: 22 January 2023

Reviewed by: Health and Care IG Panel

Common law is a form of law based on previous court cases decided by judges.

The common law duty of confidentiality means that when someone shares confidential information in confidence, you cannot disclose it without some form of legal authority or justification (a 'legal or lawful basis' in common law, **not to be confused with a legal/ lawful basis under UK GDPR).**

In practice, this means you'll need to get explicit consent from a patient before sharing confidential information collected about them when they were receiving care, unless there is another legal basis (also known as 'setting aside' the common law duty of confidentiality).

Important note reminder: this form of consent is distinct from UK GDPR consent. If the person has died without giving consent, you cannot receive the information unless another legal basis applies. It is irrelevant how old the person is, or the state of their mental health; the common law duty of confidence still applies.

Before receiving confidential patient or service-user information for your research, therefore, you will need to check that you meet 1 of the following legal bases:

- Consent, which may be implicit or explicit as follows:
  - Implied consent when no positive action is required (only relevant if you are a member of the direct care team, such that people would have a reasonable expectation of their confidential information being accessed by you)
  - Explicit consent (received from the patient **to agree to the information being shared for research purposes)**
- A legal obligation (set out in legislation or otherwise required by law, such as ordered by a judge) requiring the information to be shared
- Overwhelming public interest (this is exceptional and public interest can rarely provide a legal basis for sharing large volumes of information)
- A statutory authority or gateway that sets aside the common law duty of confidentiality: for example, support under The Health Service (Control of Patient Information) Regulations 2002 (known as 'section 251 support'). Applications to process confidential patient information for medical purposes under its regulation 5 will be considered by CAG. CAG reviews applications to set aside the common law duty of confidentiality for research purposes under section 251 of the NHS Act 2006 in circumstances when obtaining consent to share confidential patient information is not practicable. CAG then advises the HRA, which in turn determines whether an application to process confidential information without consent should be approved

For more detailed information on each of these, please read guidance from the NHS Transformation Directorate on consent and confidential patient information.

Important note reminder. The above legal bases relate to the common law duty of confidentiality only. These legal bases are different from the legal bases under UK GDPR. You should refer back to Step 4: Have a lawful basis for processing health and care data to determine which legal basis you should use to process data for research purposes under UK GDPR. You must also still comply with all other relevant legal obligations including data protection legislation and obtaining relevant research approvals before you start your research.

Regulations that govern the use of data

Deploying your digital technology: using personal health data

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: 22 January 2023

Reviewed by: Health and Care IG Panel

The processing of personal data in the delivery of care (such as in the live deployment of a healthcare technology) is for direct care. However, direct care does not encompass pre- or post-deployment testing or development of technology.

The processing of confidential patient and service-user data for direct care purposes can lawfully be made using the legal basis of implied consent under the common law duty of confidentiality. This legal basis is available to a member of the direct care team who provides care services to the individual about whom the data relates.

As explained previously, this is because patients would reasonably expect their personal data to be used for their direct care. As such, they are assumed in law to give their implied consent for their data to be shared for uses that involve prevention, investigation, or treatment of any illness involving them. That assumption remains unless the individual specifically withdraws that consent.

Direct care can be defined as a clinical, social-care or public-health activity concerned with the prevention, investigation or treatment of illness and the alleviation of suffering of individuals. It includes supporting an individual's ability to function and improve their participation in life and society. It also includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including the measurement of outcomes done by one of more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

Direct care does not include health services management, including population health management (preventative or other) initiatives, or medical research. Examples of activities that are not in-scope for direct care include risk prediction and stratification, service evaluation, needs assessment and financial audit.

Important note: whether for direct care or not, your processing must still satisfy an Article 6 legal basis, and Article 9 condition. It must also comply with the data protection principles and other compliance requirements, as stipulated by the UK GDPR. See complying with the UK GDPR.

Also see:

NHS Digital's definition of direct care

To share or not to share? The Information Governance Review

ICO's investigation into use of patient information by the Royal Free NHS Foundation Trust.

Making sure your data usage is lawful

The use of a technology in direct care does not require any further approvals or require you to obtain consent from the individuals to whom the information relates. However, as with all health data processing, data protection legislation still applies.

Regulations that govern the use of data

Post-market: compatibility of technology with existing systems

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

Reviewed by: Health and Care IG Panel

When deciding whether to buy a digital technology, potential adopters will consider whether the technology is compatible with their existing systems and infrastructure.

Thus, technology compatibility testing may be required. Again, you must make sure that your use of data during this stage is done lawfully.

Data protection criteria for compatibility testing

Although technology compatibility testing involves the use of data, it is not considered a research activity or direct care.

However, you still need to think about:

- Is the data personal or confidential?
- Who is accessing the data? For example, are they part of the care team?
- How is the data being collected, held or shared?
- What security measures are in place?

How to process data lawfully during technology compatibility testing

An already compatible technology

If a technology is already compatible with existing systems and can be integrated without processing health data, no approvals are usually required.

However, data controllers should still consider the risks from reidentification and data matching (matching data to a person).

Confidential data processed by someone within the direct care team

If confidential information needs to be processed in direct care provision, and when such information is not shared with people outside the direct care team, there is usually no need for explicit consent (to the sharing) to be in place, nor alternatively a need for section 251 (of the NHS Act 2006) support for the sharing to be requested.

Confidential data processed by someone outside the direct care team

Before confidential information is shared with someone outside of the direct care team, section 251 support for this may be required. For research purposes, and unless explicit consent to share the information has been obtained (or can be obtained) from patients and service users in advance, this will normally involve an application to the Confidentiality Advisory Group (CAG) via the HRA and HCRW to set aside the common law duty of confidentiality to permit the sharing. An example would be when manual work with the data (for example, coding) is proposed to be done by members of the technology developer's team and that would involve sharing external to the direct care team organisation.

For more information, read how to apply for research approvals in step 5 of complying with the UK GDPR.

Regulations that govern the use of data

Extra reading on data regulations

This is best practice guidance

Although not legally required, it's an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 22 January 2023

Reviewed by: Health and Care IG Panel

- The ICO's guidance on AI and data protection
- The ICO's AI and data protection risk toolkit
- The Department of Health and Social Care's guidance on digital and data-driven health and care technology
- Information governance guidance on AI, which focuses on the implications of using AI in health and care settings

