Developers guidance

# All developers' guidance



# Contents

 

Category

# Technology idea

Technology idea

# Determining if a technology is a medical device

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

Last updated: 06 November 2023

It's your responsibility as a developer to determine whether your digital healthcare technology is a medical device.

# Definition of a medical device

To decide if your digital healthcare technology is a medical device, you'll first have to compare it against the full legal definition of a medical device in the UK Medical Device Regulations 2002 (UK MDR 2002).

In summary, a medical device is any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnosis or therapeutic purposes or both and necessary for its proper application, which is intended by the manufacturer to be used for human beings for the purpose of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap
- investigation, replacement or modification of the anatomy or of a physiological process, or control of conception

A medical device does not achieve its main intended action by pharmacological, immunological or metabolic means although it can be assisted by these.

A medical device may be intended to administer a medicinal product or incorporate as an integral part a substance which, if used separately, would be a medicinal product and which is liable to act upon the body with action ancillary to that of the device.

If your technology is a software app, check GOV.UK's guidance on medical devices software applications. This gives information on how to decide whether your app is a medical device.

# Understanding medical device risk classifications

The law classifies a medical device based on the level of risk associated with it. The higher the risk, the stricter the controls on its use will be.

These are the risk classifications for general software medical devices:

Class 1 – generally regarded as low risk

 

Class 2a - generally regarded as medium risk

Class 2b - generally regarded as medium risk

Class 3 - generally regarded as high risk

The risk classification applies to the device for its given intended purpose by following the classification rules and implementation aspects of the legislation. It must be stated in all labelling and registration activities.

The risk class of your device informs:

- what regulatory processes you should follow
- the evidence you need to generate over the device's lifecycle
- whether your device needs to be assessed by an approved body or you can self-assess that it meets legislative requirements, and
- the routes of conformity through the UK MDR 2002, which are only available to certain risk classes of medical devices.

# Determining the risk classification for your medical device

When you decide your technology is a medical device, you have to determine its risk classification. This is the process of:

- reviewing and implementing the classification rules of the UK MDR 2002 against the intended purpose, and
- determining the appropriate risk classification of the medical device

To do this, you should:

- review the classification annex of the relevant legislation under the UK MDR 2002 to
  - locate the rules
  - determine which rules are applicable
- review the applicable rules against the intended purpose statement and relevant definitions, and
- follow the implementation rules within the classification annex

Misclassification of device risk may lead to compliance actions against your organisation. This could delay or stop you placing the medical device on the market, which may cost money and cause reputational damage.

 

For more information to help you determine the risk class of your medical device, see:

- the Medicines and Healthcare products Regulatory Agency's guidance on borderlines with medical devices
- the International Medical Device Regulators Forum
- our information on technical standards

# Changes to your medical device

Changes to your medical device may affect its risk classification. These include changes to the technology's intended use, functionality or the use-environment. So, you should review these and reassess your technology regularly.

Note that even if you decide your technology is not a medical device, future changes could turn it into a medical device.

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

# 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

# Writing an intended purpose statement for software medical devices

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

Last reviewed: 25 September 2024

To place your medical device on the health and social care market, you should have an intended purpose statement. You need to assess this regularly to make sure it remains fit for purpose. Changes to the intended purpose of a medical device will require regulatory reassessment.

# Understanding an intended purpose statement

Software and apps that meet the definition of a medical device must comply with the UK Medical Device Regulations 2002 (UK MDR 2002). The intended use is legally determined by "data supplied on the labelling, the instructions for use and/or the promotional materials". Creating a master intended purpose statement ensures that regulatory requirements are more easily and consistently identified and met.

Think about your medical device's intended purpose early in its lifecycle. Creating a statement will help you plan the technology lifecycle more efficiently. It will also help you follow the appropriate regulatory requirements. This should stop you wasting resources on inappropriate evidence generation.

An intended purpose statement defines who will use your medical device, how it works and who it is for.

The intended purpose statement also helps determine:

- where the medical device fits within specific care pathways
- whether it meets the definition of a medical device
- its medical device risk class, and
- the evidence that needs to be generated

If your digital technology is not a medical device, you do not need to produce an intended purpose statement. But your technology may become a medical device if you change it to meet customer needs. So, consider creating an intended purpose statement for your digital technology early in its lifecycle. This may also help when generating your value proposition.

# Creating an intended purpose statement

Use clear language and clinically-focused terminology.

 

Include these 4 key elements:

- structure and function of the device
- intended population
- intended user
- intended use environment

It is your responsibility as the developer to determine what level of detail is required for each of the elements. It is important to note that the MHRA interprets the elements of an intended purpose as broadly as possible and from the stance of an objective observer.

Think about whether you will be able to generate clinical evidence to demonstrate your device meets the specifics of the intended purpose. If not, then your intended purpose is likely to be unsuitable.

For more information, see crafting an intended purpose in the context of Software as a Medical Device from the Medicines and Healthcare products Regulatory Agency.

## After you have written your intended purpose statement

The intended purpose statement forms part of your medical device's technical documentation.

Depending on the device's risk classification and your chosen route to market, you may need to make a submission to an approved body. If so, you will include the intended purpose statement in the submission documents for review alongside the provided clinical evidence to ensure adequate alignment.

The MHRA encourages you to make your intended purpose statement publicly available. This transparency will help you when engaging with regulators, adopters and the wider health and social care system.

# What happens if the intended purpose changes?

There may be changes in the clinical pathway, the requirements of end users and patients, or the functionality of your medical device. These may affect the intended purpose.

 

If so, you will have to update the intended purpose statement and supporting evidence.

Changes to your medical device's intended purpose statement will need a review by your approved body, where applicable. This may require reassessment of the documentation if the change is significant enough to alter the original risk-to-benefit assessment.

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

# Aligning the intended purpose and value proposition of your digital technology in health and social

### 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)
- National Institute for Health and Care Excellence (NICE)

Last reviewed: 25 August 2022

Aligning the intended purpose and value proposition of your digital technology is vital to placing your technology on the health and social care market.

# Risks of not aligning the intended purpose and value proposition of your digital technology

To place your digital technology on the health and social care market, you need to:

- define and document the intended purpose of your technology
- outline and document its value proposition and
- make sure the 2 align

Aligning your intended purpose and value proposition helps make sure you collect appropriate evidence and comply with the appropriate regulatory checks.

Not aligning the intended purpose and value proposition might:

- suggest to regulators, health technology assessment bodies or adopters that you have not understood your technology's regulations or have not complied with them
- raise doubts about the safety and effectiveness of your technology, because it suggests you have not done the regulatory checks appropriate to its intended purpose. This means the technology could have safety issues
- risk wasting resources on inappropriate evidence generation. You could be required to retrospectively generate further evidence, which would delay placing your product on the market

Align the intended purpose and value proposition at an early stage, ideally during technology conceptualisation. This will make sure you follow the correct regulations. Regularly review both documents throughout the lifecycle of your digital technology, especially if your technology changes. This will help you place your technology on the health and social care market.

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

# Understanding UK MDR 2002 regulations for medical devices

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

To place a medical device on the market, there are certain requirements you need to meet.

# Medical devices: Complying with UK law (UK MDR 2002)

UK law specifies requirements that legal manufacturers of medical devices must meet to legally place a device on the market.

These requirements are set out in the UK Medical Device Regulations 2002 (UK MDR 2002). They apply to all digital technologies meeting the definition of a medical device in the UK.

The regulations make sure that medical devices placed on the UK market are safe and effective for patients, the public, and health and care professionals.

Understanding these regulations will help you to plan the development of your medical device more effectively and avoid wasting time and resources.

Medical devices that comply with the law encourage public trust. This has a positive effect on adoption rates and investment in innovation.

Non-compliance can lead to:

- prosecution
- removal of your device from the market
- delays in development and adoption of your device
- damage to your reputation

# How to make sure you conform with the UK MDR 2002

You should start thinking about the UK MDR 2002 during the conceptualisation stage of your device. This will help you plan for compliance, engineering and evidence generation. If your digital technology is considered to be a medical device ('in scope') the requirements of the legislation apply throughout its entire lifecycle.

 

## Step 1: what parts of the UK MDR 2002 apply

Determine which parts of the legislation in the UK MDR 2002 applies to your device when defining its intended purpose.

This could be:

- Medical Devices
- Active Implantable Medical Devices, or
- In Vitro Diagnostic Devices

## Step 2: medical device documentation

Think about how to show that your device conforms with the essential requirements of the relevant legislation. This is done by creating and maintaining documentation and processes based on the risk classification of the device and the conformity route that you choose.

## Step 3: medical device assessment

Consider how your device will be assessed. For low-risk devices (Class 1), you will be able to self-certify. Higher-risk devices (Class 2a, 2b and 3) and class 1 devices with additional considerations (such as a measuring function) are assessed by an approved body. These approved bodies are governed by the same legislation and overseen by the Medicines and Healthcare products Regulatory Agency (MHRA).

Successful assessment will allow you to assign a UKCA mark to your device. You will declare that to the best of your knowledge its benefits outweigh the risks, which have been minimised.

# Is your digital technology a medical device?

Think about how close your technology is to being a medical device, even if it does not currently meet the criteria. Your technology may become a medical device if functionality is added over time. An example would be added functionality in response to changes in user requirements if used in a slightly different population. Be aware of this possibility and plan for it in your technology development strategy.

 

# Resources:

Stay up to date with the MHRA's latest guidance on regulating medical devices in the UK.

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

# Planning for management systems, including a quality management system (QMS)

### This is required guidance

It is legally required and it is an essential activity.

### This Guide covers:

- Great Britain (England, Scotland, Wales)

### From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

If you're developing medical devices, you're legally required to implement a quality management system (QMS). If you're developing non-medical devices, implementing a QMS is not legally required, but is essential to market access.

# Build and certify management systems

To show compliance with regulations, you need to build management systems. You also may need to certify them.

These are internal processes and policies that ensure:

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

The breadth and extent of your management systems depend on your specific objectives. For example:

- when developing a medical device, you may have the objective of achieving high device quality and can work towards this using a QMS
- when working with sensitive data, you may use an Information Security Management System (ISMS) to manage your objectives for data security and handling

# What is a quality management system?

When developing medical devices, you're legally required to implement a Quality Management System (QMS). A QMS outlines processes that minimise the risks associated with the production, deployment and surveillance of medical devices. A robust QMS provides structure for key company processes around device safety and efficacy.

Adopters may ask you for proof of certification by an approved or notified body against a relevant standard. This will increase assurance that you meet the standard. For example, when developing medical devices, you should be able to provide an up to date and in-scope certificate against ISO 13485 to prove a conforming QMS.

As a medical device developer, you are legally required to have this QMS and do activities which, depending on scope, may include:

- design and development

 

- evidence generation
- post market surveillance

A QMS built to ISO 13485 requirements provides:

- document management (version control, long-term storage and standardised structure)
- risk assessment
- sign-off procedures
- decision records

Your QMS is as much a way of working as it is a tool for compliance. It should evolve in line with company aspirations and throughout the lifecycle of the technology.

# Setting up a Quality Management System

Review all relevant ISO standards when designing and building your systems and processes, and determine which ones are useful for your specific needs.

You may decide to implement several management systems or combine their attributes to meet different needs. For example, using a manufacturing quality system for a medical device or an information security system for data management.

The core principles in many management systems are similar but they focus on different aspects, and some need higher levels of rigour and evidence during auditing.

Consider using a consultancy service to support you in designing, building and auditing your management systems.

Use your management systems throughout the whole lifecycle of your technology and audit them frequently. If you have a quality management system (QMS), it will be periodically reviewed by the approved body.

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. For medical devices, a QMS needs to be in place and certified before you finish developing your device.

 

# Resources:

Review the relevant standards for creating a QMS, including:

ISO 13485 medical devices

ISO 14971 application of risk management to medical devices

ISO/IEC 27001 information security management

BSI Standards catalogue

IEEE SA Standards

IEC Standards

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

# 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

# Understanding routes to NICE health technology assessment

### 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: 07 April 2025

Last updated: 07 April 2025

Understand how NICE does health technology assessments.

# Planning for a NICE evaluation

NICE evaluates and produces guidance on many new products for the health and social care services in England. This includes digital health interventions, medical devices and diagnostics.

Your digital technology could be eligible for a NICE evaluation. Planning for a NICE evaluation in your evidence generation plans may:

- increase the likelihood of a positive recommendation by NICE. This will increase the likelihood of adoption of your technology across the NHS
- reduce delays in adoption of your technology
- help you create evidence generation plans that support your value proposition.

A key step in early planning is finding out about NICE's topic selection process and how guidance topics are prioritised.

Adopters may use NICE evidence standards when deciding whether to buy your digital technology. They may particularly use NICE's evidence standards framework for digital health technologies.

So it is important to consider these, even if your technology is not evaluated by NICE. For more details, see generating evidence for health technology assessment.

# NICE evaluation: how does it work?

NICE carries out evaluations through a range of programmes, which require different evidence. The HealthTech programme is responsible for evaluating digital technologies and AI technologies, as well as traditional medical technologies, diagnostics and interventional procedures. The type of assessment that is done by NICE depends on the type of technology and the stage of development. The HealthTech programme has a methods and processes manual that explains how guidance is developed.

## The HealthTech programme assessments are:

- interventional procedure guidance (IPG) which recommends whether an interventional procedures, such as laser treatments for eye problems or deep brain stimulation for chronic pain, are effective and safe enough for use in the NHS.

 

- early use assessment, which is a quick assessment of technologies for clinical effectiveness and value for money. It assesses technologies at an early stage in evidence generation and recommends promising technologies for use in the NHS, while further evidence is being collected.
- Routine use guidance, which assesses products that have not been adopted widely but have substantial evidence to produce guidance in favour or against.
- late-stage assessment for categories of technologies that are already being widely used within the NHS.

The HealthTech programme has independent committees that review the evidence for each technology and make recommendations about using them in health and social care.

Topics are selected by NICE's prioritisation board to ensure they reflect national priorities for health and care. Typically, any technologies within these topics that are eligible for a NICE evaluation will need to:

- have a CE or UKCA mark
- be a tier C intervention within NICE's evidence standards framework for digital health technologies, and
- have enough evidence to support the value proposition

# Get your digital technology a NICE evaluation

Register with the NHS Innovation Service to find out if your technology could be eligible for a NICE evaluation.

Generate your evidence in line with NICE's evidence standards and methods guides, such as:

- NICE's HealthTech programme manual (in development)
- NICE's evidence standards framework for digital health technologies
- NICE's real-world evidence framework

Consider using NICE Advice.

 

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 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

# Evidence generation when your digital technology is relevant to a national screening programme

## This is best practice guidance

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

## This Guide covers:

- United Kingdom

## From:

- UK National Screening Committee (UK NSC)

Last reviewed: 25 September 2025

Last updated: 25 September 2025

If you're developing screening tests for the NHS, you will need to generate specific evidence which meets a higher bar.

# Why are screening services different, and why should I generate specific evidence for them?

The NHS website lists the NHS population screening programmes. The advice below refers to screening programmes provided by the NHS only, not to private providers.

Many digital technologies can be used in both diagnosis and screening pathways for the same disease areas. Take the use of mammograms in breast cancer as an example.

Mammograms are used in screening pathways for breast cancer, in which women in a specific age bracket are invited for breast checks. They are also used in diagnosing cancer when a patient presents with symptoms to their GP. This includes women outside the screening age bracket and men with breast cancer symptoms.

People coming for screening tests will be different from people showing up with symptoms. This means the technology may be more or less effective for these different groups. So, the evidence requirements will be different.

An NHS population screening programme may have different evidence requirements than, for example, a service for symptomatic patients in an NHS trust or clinical commissioning group. This is because screening programmes invite healthy people in for a screening test. Because getting it wrong can lead to a healthy person coming to harm, the NHS population screening programmes set high evidence standards before making changes. So, you may have to generate evidence which meets a higher bar. If you do not think this through early on, you will likely have problems. These include:

- getting the marketing authorisation for your technology with the appropriate intended use so that it can be considered in an NHS screening population. For example, if a programme uses nurse practitioners instead of doctors to do screening tests, your medical device's intended purpose will need to be for that type of care professional
- generating appropriate evidence for a national screening programme, which could result in your company's resources or time being wasted on misdirected research

 

# What does the UK National Screening Committee do?

Screening programme policy is informed by the expert, independent advice of the UK National Screening Committee (UK NSC). It advises governments across the 4 UK nations on whether new screening programmes should be recommended, what should be included as part of established national screening programmes and whether they should be changed or not. This includes making any major modifications to them such as using a new test that includes AI or digital technology.

The UK NSC reviews peer-reviewed evidence for a technology's effect on the clinical pathway. It will not only take interest in technical accuracy but also downstream resource and impact implications, such as:

- the clinical impact of the screening test on other parts of the pathway such as screening uptake. For example, an invasive screening test might put some people off participating in screening
- the number of patients unnecessarily referred from the screening programme to treatment services, which risks overdiagnosis and overtreatment
- workload and resource requirements
- social and ethical issues. This includes whether a given screening test is more or less effective in a particular demographic group, especially if it is a marginalised group
- patient and clinical acceptability

# What do I need to do?

## Step 1: Determine whether your digital technology is relevant to national screening programmes and might be evaluated by the UK NSC

The UK NSC evaluates any proposed alteration that constitutes a 'major change' to a screening programme. This might include:

- introduction of an alternative screening test to replace the current primary screening test
- introduction of an additional test in the pathway
- evidence of altered cost effectiveness or cost

 

The UK NSC does not need to review changes when a technology is used to improve the operational delivery of the existing screening programme pathway (for example, improvements to administration processes). This is because these do not alter the patient's pathway of care.

However, these are not always 'black and white'. For example:

## Step 2: Learn about the UK NSC's evidence requirements and processes

You can learn about this by reading:

- this blog from Public Health England
- section 5.4 of the UK NSC evidence review process

You should also review the UK NSC recommendations on population screening for a condition using previously evaluated technologies. These set out the state of the science at the point of publication and highlight areas in which further research is needed. For example, the UK NSC published a review on use of AI in breast cancer screening. This was followed up with an article in the Lancet addressing important considerations in research into the use of AI in breast cancer screening.

## Step 3: Plan your evidence generation

If you intend to do research within an NHS screening service, you should seek advice from a programme-specific research advisory committee (RAC). RACs advise on the feasibility of proposed changes to a screening programme and review evidence-generation plans. They are hosted by the NHSE Public Health Commissioning and Operations Team.

If you are developing technology with a value proposition relevant for diagnosis of a disease in symptomatic patients and for use in asymptomatic people in a screening pathway, you should research the evidence requirements for both pathways.

You should also make sure this aligns with your technology's intended use. For example, a screening programme might have nurse practitioners screen patients because this is clinically and cost effective. But if the intended use of your technology as per its marketing authorisation is for consultant doctors in secondary care only, it cannot be used by nurse practitioners. If so, you might need to do another clinical trial to get this marketing authorisation.

 

## Step 4: Determine the type of proposal you need to submit

Consider whether you are:

- proposing a new topic
- requesting an early update for a topic
- suggesting a modification to an existing screening programme

Check the UK NSC recommendations to determine the current status, if any, of the topic.

## Step 5: Submit your evidence and proposal to the UK NSC

The UK NSC previously invited stakeholders to submit proposals during a 3-month period between 1 July and 30 September each year.

This open call for topics process has been updated and now follows a 2-year cycle.

- The next open call is scheduled to run from 1 July 2026 to 30 September 2026 as announced in the UK NSC blog.
- An exceptions process will allow the UK NSC to consider proposals outside the new 2-yearly open call period if there is significant new evidence that meets specific criteria.

For more information read how to submit a proposal to the UK NSC

**When do I need to consider this?**

You need to learn about the screening programmes and the process for submitting for a major change during technology conceptualisation. This is because you should have a clear value proposition for your technology before you decide on its intended purpose, which then informs your approach for gathering evidence to apply for a UKCA mark.

But the work to demonstrate your value proposition and generate evidence for the UK NSC will start during the technology development stage.

For examples of UK NSC evidence reviews, see:

- use of AI in breast cancer screening: rapid review and evidence map
- automated grading in diabetic eye screening: rapid review and evidence map

 

Technology idea

# Complying with Ionising Radiation (Medical Exposure) Regulations (IR(ME)R)

### This is required guidance

It is legally required and it is an essential activity.

### From:

- Care Quality Commission (CQC)

### This Guide covers:

- England

The Ionising Radiation (Medical Exposure) Regulations (IR(ME)R) provide a framework for the safe use of ionising radiation in medical and non-medical imaging, including use of medical devices. Only appropriately qualified and trained human operators can be responsible for the clinical evaluation of any ionising radiation exposure. Legally, AI and data-driven technologies cannot replace human decision making and should only support it.

# Ionising radiation and medical devices

The Care Quality Commission (CQC) enforces the Ionising Radiation (Medical Exposure) Regulations (IR(ME)R).

These regulations aim to make sure that medical ionising radiation is used safely to protect patients from the risk of harm.

IR(ME)R sets out the responsibilities of duty holders for radiation protection and the basic safety standards that they must meet. Duty holders include the:

- employer
- referrer
- practitioner, and
- operator

You can find these regulations in the:

- Ionising Radiation (Medical Exposure) Regulations 2017
- Ionising Radiation (Medical Exposure (Amendment) Regulations 2018

 

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

# UKCA marking requirements for medical devices

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

Last reviewed: 13 January 2025

To place a medical device on the market in England, Wales or Scotland you must show it meets certain regulations.

# Why you need a UKCA mark

The UK Conformity Assessed (CA) mark shows your device meets the requirements of the UK Medical Device Regulations 2002 (UK MDR 2002). If you do not know whether your technology is a medical device, read determining if a technology is a medical device.

You should get a UKCA or relevant CE mark before placing a medical device on the market in England, Wales or Scotland. This is required by law. Different legislation is in place for medical devices in Northern Ireland – see GOV.UK for regulation of medical devices in Northern Ireland.

If you do not comply with the UK MDR 2002, the Medicines and Healthcare products Regulatory Agency (MHRA) has enforcement powers to hold you accountable. Serious non-compliance can result in criminal prosecution and civil sanctions against you. The MHRA also has powers to remove unsafe devices from the market.

# Getting a UKCA mark

To get a UKCA mark for your medical device you should:

- work out the risk classification for your device
- read all the relevant legislation that applies to your class of device
- generate evidence and documentation, and
- prove you've met the requirements

If you do not know the risk class for your device, see determining if a technology is a medical device.

## Identifying which requirements are relevant to your device

To get a UKCA mark you must meet the essential requirements relevant to your device in the UK MDR 2002. You should identify which regulations apply to the intended use of your device.

 

The 3 main types of medical devices and their requirements are:

- General medical devices – see Part 2 of the UK MDR 2002
- Active implantable medical devices – see Part 3 of the UK MDR 2002
- In vitro diagnostics medical devices – see Part 4 of the UK MDR 2002

## Proving you've met the requirements

You must prove your medical device meets the relevant requirements. You do this by providing a declaration of conformity. You can self-assess for a Class 1 device. But higher-risk class devices must have a conformity assessment done by an approved body.

## Having a conformity assessment

The type of conformity assessment depends on the risk class for your device.

Use the conformity assessment routes guide on GOV.UK to find the route to conformity assessment for your class of device. For the purposes of this guide, read:

- 'CE marking' as 'UKCA marking'
- 'Competent Authority' as 'MHRA'
- 'Notified body' as 'approved body'

There are several approved bodies in the UK that you can choose from. Make sure your chosen body is qualified and experienced in certifying devices of your class. You can search the register of UK conformity assessment bodies to find an appropriate body.

## Preparing for the conformity assessment

You must create documentation that references each requirement and how you've met it. You can create most of this documentation from your Quality Management System (QMS) processes. If you've not set up your QMS, do it before or in parallel with the device documentation. This makes sure you use systematic approaches.

You must show evidence of:

- Processes
- Risk management systems
- Device design
- Device development
- Clinical evaluation

 

You must follow the regulations before placing your device on the market.

# After passing your conformity assessment

Once you've passed your conformity assessment, you'll receive a certificate from your approved body.

After you get your certificate, you should:

- place the UKCA mark on your device
- place the identification number of the approved body on your device, and
- register yourself and your device with the MHRA

If your device changes after it's been placed on the market, you must reassess to make sure you're still meeting the requirements.

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 development

# Creating and maintaining quality management systems for medical devices

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

To meet the requirements of the law you need to create and maintain quality management systems (QMS) for medical devices. ISO 13485 QMS defines the requirements you must meet.

# Creating and maintaining a quality management system for medical devices

To meet the requirements of the UK Medical Device Regulations 2002 (UK MDR 2002), developers of medical devices must create and maintain a quality management system (QMS).

A QMS is a series of processes and documents in the form of policies, standard operating procedures and records. These specify the objectives, ways of working and results of your activities. Follow the standards of the ISO 13485 QMS to make sure you are doing it properly.

The aim of a QMS is to:

- mitigate risks
- improve consistency
- improve efficiency
- create safe high-quality medical devices

Building, certifying and maintaining a QMS can cost a lot of time and money. This depends on your existing expertise, the complexities of the QMS and the capacity of approved bodies. Factor this into your development plans early to reduce significant delays later.

# Following ISO 13485 QMS standards

## Step 1: Read ISO 13485:2016 medical devices – quality management systems

ISO 13485:2016 quality management systems standard specifies the requirements of a QMS system for the development of medical devices.

 

## Step 2: Get ISO 13485 certification

Schedule auditing by an approved body which, if successful, will grant certification against the standard.

## Step 3: Maintain the QMS system

Use your QMS throughout the whole device lifecycle and audit it frequently. It will be periodically audited by your approved body.

Note that the scope of your QMS may vary depending on the specific activities done during the lifecycle of the device. You must ensure that all activities you require are included in your scope and audited against. But remember, the scope of your QMS needs to be defined prior to getting assessed and certified. You cannot change the scope of the QMS without getting reassessed by your approved body.

For example, some companies outsource their design activities to another organisation. In which case, each organisation should have a separate QMS. Their remit and scope will cover different processes and have defined processes for the 2 organisations interacting.

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 development

# Meeting risk-management requirements for medical devices

### This is required guidance

It is legally required and it is an essential activity.

### This Guide covers:

- Great Britain (England, Scotland, Wales)

### From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

To deploy a compliant healthcare technology safely, you need to implement a risk management system. ISO 14971:2019 sets the requirements for risk management systems for medical devices.

# Complying with UK MDR 2002 risk management

Understanding how to manage risk is a key component of meeting the legal requirements of the UK Medical Devices Regulations 2002 (UK MDR 2002).

The UK MDR 2002 and the quality management systems (QMS) standards, ISO 13485, require developers to evaluate the risks of a given process, device component or scenario.

The core aspects of risk management are considered best practice. They are widely used in healthcare to assess:

- clinical safety
- data and information governance
- cybersecurity
- medical device safety

ISO 14971 provides the requirements you need to meet for the risk-management aspects of the UK MDR 2002 and ISO 13485.

# Taking a risk-based approach when developing medical devices

Risk management is a structured way of assessing situations, processes and devices to:

- identify, analyse and quantify risks
- mitigate unacceptable risks
- justify residual risks

To meet the legislative requirements of the UK MDR 2002, you must make assessments and design decisions taking a risk-based approach. This shows that decisions are made in a proportional manner. It also makes sure you identify the overall device risks and show they are outweighed by the expected benefits.

 

There are several risk-management approaches and tools you can use, depending on your medical device and how it will be used.

# How to take a risk-based approach when developing medical devices

Refer to ISO 14971:2019 medical devices – application of risk management to medical devices.

This standard provides the requirements to meet the risk-management aspects of both the UK MDR 2002 and the QMS standard ISO 13485.

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 development

# Meeting design requirements for medical devices: meeting UK MDR 2002

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

To meet UK regulations, you need to show you've designed medical devices to the appropriate safety standards.

# Designing medical devices to appropriate standards

The Medical Devices Regulations (UK MDR 2002) state that you must design and develop medical devices to meet the safety requirements.

Creating and maintaining design and development documents makes compliance and operational tasks more robust.

The documents form part of the device's technical file, which is used to prove you're complying with regulations. The technical file will also include your clinical evidence and risk-management documents.

Design documents are crucial in further development work, failure investigations and company growth. They make sure that device knowledge and quality-control processes are maintained as you progress through the device's lifecycle.

Creating design documents mostly happens in the development stage. However, user needs are typically generated in the conceptualisation stage. So, the documents must be kept up to date throughout the device's lifecycle.

# Included in the design documents

To prove you're meeting the design requirements of the UK MDR 2002, you need to create version-controlled documents containing the design and development information for your medical device.

Exactly what documents are produced varies between medical devices. It depends on factors such as the complexity of the device and the development process. Typical documentation may include:

- describing what the device looks like at a technical level (for example, architectural diagrams and schematics)
- information on suppliers of components not made in-house
- defining the user needs for development of functionality
- design inputs and outputs from the development process; that is, the target functionality and result achieved after development

 

- verification and validation information relating to original user needs
- risk management and clinical-evidence documentation
- a record of design changes and testing to demonstrate maintained or improved functionality

The Quality Management System (QMS) you design to meet ISO 13485:2016 standards will help you generate these regulatory documents. They are created in line with best-practice standards.

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 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

# Determining whether a clinical investigation is needed for medical devices

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

To get a UKCA mark for your medical device, you may need to prove its safety through a clinical investigation. Here's how to get the required approvals for the clinical investigation of medical devices.

# Clinical investigation of medical devices: what it is and why you need one

To apply the UKCA mark to a device, you must prove it meets the essential requirements of the Medical Devices Regulations (UK MDR 2002). To do this, you may need to provide clinical data through a clinical investigation to support the clinical evaluation process.

## A clinical investigation

A clinical investigation is a specific type of prospective clinical trial of medical devices that do not have a UKCA mark. It is done to prove the safety and performance of medical devices under normal conditions within the intended use.

## Clinical data

The clinical data you need might come from various sources. It might come from a critical evaluation of relevant scientific literature. You may be able to use clinical data from equivalent compliant devices to confirm the clinical safety and performance of your medical device.

Using clinical data and clinical evidence from equivalent devices will save you time and avoid redundant clinical investigations.

In this scenario, you'll need to show clinical, technical and biological equivalency.

Alternatively, an evaluation of the data produced by a clinical investigation or a combination of the 2 approaches can be used.

# MHRA and HRA approvals

A clinical investigation must have approval from the Medicines and Healthcare products Regulatory Agency (MHRA) and the Health Research Authority (HRA) before it can start. This includes independent ethical opinion from a Research Ethics Committee.

 

The MHRA assessment process takes up to 60 days with a result of objection or no objection given by the end of this period. HRA approval takes about 40 days.

# Clinical data for AI-driven digital technology

Analysis and evaluation of scientific literature are broad concepts. And in the case of AI-driven digital technology it may be difficult to use clinical data from equivalent compliant medical devices. This is because there is likely to be variation in the training data used between devices.

**So it is likely you'll need to do a clinical investigation of the medical device to answer outstanding questions about safety and performance.**

If a clinical investigation is not done, you may not be able to prove that the device meets the essential requirements. This could become a compliance issue and cause delays, prison sentences or fines.

# Getting approvals for the clinical investigation of medical devices

## Step 1:

Notify the MHRA in advance of your intention to apply for permission by emailing information to mhracustomerservices@mhra.gov.uk.

This should include:

- basic details of the device
- intended population
- type of study
- estimated timelines

Follow guidance on how to notify the MHRA about a clinical investigation for a medical device on GOV.UK.

 

## Step 2:

Create your application on the Integrated Research Application System (IRAS). This is a single system for applications to both the HRA and the MHRA.

## Step 3:

Pay the fee listed in the current MHRA fees on GOV.UK.

## Useful resources:

ISO 14155:2020 Clinical Investigations of medical devices in human subjects – good clinical practice.

Clinical evaluation: a guide for manufacturers and notified bodies under directives 93/42 and 90/385 (MEDDEV 2.7/1 revision 4)

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 development

# Demonstrating clinical performance of medical devices with a Clinical Evaluation Report (CER)

### This is required guidance

It is legally required and it is an essential activity.

### This Guide covers:

- Great Britain (England, Scotland, Wales)

### From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

To get a UKCA mark for medical devices, you need to include a Clinical Evaluation Report (CER) in your application documentation.

# Clinical performance and why it's important

To meet the essential requirements of the Medical Devices Regulations (UK MDR 2002), you need to prove that your medical device is safe and effective. This will relate to the intended use of your medical device.

Demonstrating clinical performance will help you gain a UKCA mark. It will also provide the foundation for marketing materials and support discussions with potential customers.

If you do not show adequate clinical performance, you will not get a UKCA mark.

# Medical devices: how you demonstrate clinical performance

You need to produce a Clinical Evaluation Report (CER) to demonstrate clinical performance.

The CER is a living document that you'll need to keep up to date throughout the lifecycle of your medical device. It includes the evidence used to prove that the benefits of medical devices outweigh the risks of using them.

The CER is produced and maintained by following the structured process of 'clinical evaluation'. During clinical evaluation, you need to demonstrate scientific, analytical and clinical validation.

Meeting these requirements is achieved through a variety of means including (but not limited to):

- defining the 'state of the art' through a literature review
- in-house testing
- prospective premarket trials
- post-market clinical follow-up studies

 

The complexity of creating the CER is related to the medical device, and it's intended use. So, an intended use statement will help you to clearly identify the evidence requirements you need to meet the regulations. Remember, you can only get a UKCA mark by showing adequate clinical performance.

The CER must be reviewed periodically and updated to represent changes in the state of the art and evidence relating to the device.

You can use the following guidance to support you in doing a clinical evaluation:

- International Medical Device Regulators Forum – Software as a Medical Device (SaMD): Clinical Evaluation
- MEDDEV 2.7/1 rev4 Clinical Evaluation: Guide for manufacturers and notified bodies
- Guidance MEDDEVs

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 development

# Generating evidence for NICE health technology assessment

### 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 November 2023

Last updated: 02 November 2023

If you want NHS England to adopt your digital technology, undergoing a NICE health technology assessment can help. Here is what you need to consider.

# NICE health technology assessment

The National Institute for Health and Care Excellence (NICE) provides guidance to NHS England on the clinical and cost effectiveness of selected new and established digital technologies. To do so, NICE carries out appraisals of digital technologies at the request of the Department of Health and Social Care.

If your digital technology is eligible for a NICE evaluation, you'll need to generate evidence that supports your value proposition. Doing so will increase the likelihood of a positive recommendation by NICE. This will increase the likelihood that the NHS will adopt your technology.

# Evidence for NICE health technology assessment

You'll need to show NICE that your digital technology is:

- clinically effective
- safe, and
- cost effective

Some of this evidence will be identical to the evidence required to get a UKCA mark.

However, as a general rule, evidence to get a UKCA mark is more focused on the safety and efficacy of your digital technology. Efficacy evidence determines whether your technology produces the expected result under ideal circumstances.

On the other hand, evidence for NICE or adopters is more focused on relative effectiveness**.** Relative effectiveness evidence measures the degree of beneficial effect compared with the current standard of care. So you will need to prove that your digital technology is effective, in comparison with current routine practice. The key is to make sure your study reflects what happens in current clinical practice as closely as possible. For example, you should aim to recruit a population that closely matches the population who would use your technology in routine practice. And when selecting sites in which to test your technology, make sure you select ones that reflect established practice in the wider health and care system.

 

# Proving your digital technology is clinically effective

If your technology is aimed at improving patient outcomes, it is essential to collect data on the most important and relevant outcomes for patients. Relevant outcomes are those that measure how a patient feels, functions or survives. The choice of outcomes to measure is also specific to the purpose of a technology. For example, a technology aimed at diagnosing cancer may need to collect longer-term patient outcomes such as cure rate or progression-free survival. You'd also need to gather diagnostic accuracy data for the technology.

A key element of clinical-effectiveness and safety data is having a long enough follow-up time to capture all relevant outcomes. For example, if your technology is aimed at improving survival in cancer patients, your study may need longer-term follow up. Or it may need to capture appropriate intermediary outcomes that can predict longer-term survival.

The quality of a study's overall design, how it is done and its validity will also be reviewed by NICE and adopters. Critical appraisal is usually done to assess the quality of your evidence.

Typically, evidence will be critically appraised in line with the relevant risk-of-bias tool for that study design. For example, the Cochrane risk-of-bias tool for randomised trials.

See using PICO to generate evidence for AI development for further guidance on generating appropriate evidence.

# Proving your digital technology is cost effective

You will also need evidence of different levels of cost effectiveness. This will depend on:

- the type of digital technology
- how a digital technology compares to current practice

 

## Digital technology: same or better performance at similar or lower cost

You will need to do a cost-consequence analysis if your technology offers:

- the same clinical effectiveness as current practice
- better performance than current practice but at a similar or lower cost.

This type of analysis will set out all the relevant costs and consequences of using your technology. It also estimates the resource use and clinical benefits of your technology compared with current practice.

## Digital technology: better performance at higher cost

If your technology offers better performance at a higher cost, a cost-utility analysis (CUA) is needed.

Processing data on costs and resourcing of your technology is essential regardless of the type of economic evaluation that will be needed.

# How to generate evidence for a NICE health technology assessment

Generate your evidence in line with NICE's evidence standards and methods guides, such as:

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

Consider using NICE Advice. NICE Advice can help you demonstrate the value of your product and make valuable NHS connections, speeding up patient access to the best treatments and care.

NICE will also consider the quality of the data you have used when training, testing and validating your algorithms. See data quality considerations when training, testing and validating your algorithms for more information.

 

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

# What it means to place medical devices on the UK market

### This is required guidance

It is legally required and it is an essential activity.

### This Guide covers:

- Great Britain (England, Scotland, Wales)

### From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

Last reviewed: 25 September 2024

Entry into the UK health and social care market can be challenging for developers of digital technologies driven by data and AI. What does ‘placing a technology on the market’ mean in relation to medical devices?

In the context of medical devices, placing a product on the market means making it available for use in the context of its intended purpose. its intended way. This includes devices provided for free.

To place medical devices on the market, you may need to advertise them directly to consumers and adopters. These could be local and/or national commissioners.

Once medical devices are placed on the market, they are subject to UK legislation relating to post-market surveillance and monitoring. Additionally, medical devices placed on the UK market are required to register with the MHRA.

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.

 

Placing a technology on the UK market

# Registering medical devices with the MHRA

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

Last reviewed: 25 August 2022

Before you place medical devices on the market, you should register each device with the MHRA. Here's how.

# Registering medical devices: why developers should do it

Registering your medical device with the MHRA is a legal requirement of the UK Medical Device Regulations (UK MDR 2002). Registering proves that medical devices comply with relevant regulation. You should register with the MHRA for each device you place on the market. If you are not in the UK, you should appoint a UK Responsible Person to do it for you.

Compliant devices encourage public trust, which has a positive effect on adoption rates and investment in innovation.

Non-compliance can lead to:

- prosecution
- removal of your device from the market
- delays in development and adoption of your device
- damage to your reputation

# How to register medical devices with the MHRA

Register your medical device with the MHRA here. You should do this before placing your device on the market. You will have to pay a fee and may also apply to make amendments.

# Registering medical devices if you are outside the UK

If you're a developer based outside the UK and wish to place a device on the Great Britain market, you should appoint a single UK Responsible Person who will take responsibility for the device in Great Britain. This applies only to developers in England, Scotland and Wales.

 

Doing this shows you are compliant with medical device regulations. You should do this before placing your device on the market.

Get further detail on the UK Responsible Person here.

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 gov.uk for information on the MHRA's enforcement duties.

 

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

# Post-market surveillance of medical devices

## This is required guidance

It is legally required and it is an essential activity.

## This Guide covers:

- Great Britain (England, Scotland, Wales)

## From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

Last reviewed: 14 July 2023

Last updated: 14 July 2023

After your medical device is placed on the UK market, you should monitor the device and report any safety incidents to the MHRA. This is known as post-market surveillance.

# Why you should do post-market surveillance

Post-market surveillance makes sure your device is acceptably safe to use for as long as it is in use. If you do not follow the requirements the MHRA may prosecute you. This could result in 6 months in prison or an unlimited fine.

# How to do post-market surveillance

## Make sure your quality management system is set up appropriately

You should collect and analyse data on the performance and safety of your medical device in a systematic manner. You will use your quality management system to help you do this. Having this system in place is a core part of medical device safety. So, it's important to make sure the system is set up appropriately.

Your quality management system will likely need:

- processes for collecting information (for example, feedback or complaints from users and audit findings)
- analytical methods to assess collected data and identify reportable incidents
- procedures and systems for investigating the cause of safety concerns and implementing corrective actions
- tools to trace and identify the device in case corrective actions are needed (for example, traceability of a potentially defective device so it can be recalled)

See our guidance on planning your quality management system and the relevant standards you should follow to create it.

## Identifying an adverse incident

A safety concern is deemed to be a reportable adverse incident when it meets these 3 criteria:

- an event has occurred

 

- the device is suspected to be a contributory cause of the event
- the event resulted in, or may have resulted in, death or a serious deterioration in the state of health of a patient or person

Note that an 'event' is not limited to use of the device by or for a patient. An 'event' includes device testing, examination of supplied information or wider scientific information that could lead or has led to an event.

Not all reportable events result in direct harm from the situation or an intervention. An event is still reportable if no injury was sustained but could occur if the event is repeated.

## Reporting an adverse incident to the MHRA

You should notify the MHRA as soon as you become aware that your device may have caused or contributed to a reportable incident. Report individual incidents on the MORE portal.

Each individual report must lead to a final vigilance report, unless you combine the initial and final report into one report. The final report should include your root cause analysis and details of any similar incidents that have occurred, along with the corrective or preventative measures that you took.

You can find guidance on how to analyse the root cause in ISO 14971.

Some adverse incidents can be submitted as part of periodic summary reporting. You would have to arrange details of the timing and content of periodic summary reports on an individual basis with the MHRA.

For more information on the vigilance system and what constitutes a reportable incident, see the MHRA's guidance on vigilance.

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 in use

Post-market surveillance of medical devices

# Identifying adverse incidents for Software as a Medical Device

### This is required guidance

It is legally required and it is an essential activity.

### This Guide covers:

- Great Britain (England, Scotland, Wales)

### From:

- Medicines and Healthcare products Regulatory Agency (MHRA)

If your technology is Software as a Medical Device (SaMD), indirect harm is the most probable outcome of an adverse incident. It is important you understand types of indirect harm and how it is caused, so you can identify adverse incidents.

# Identifying adverse incidents

Indirect harm from using SaMD may be a consequence of:

- the medical decision
- action taken or not taken by healthcare professionals based on information provided by the SaMD
- action taken or not taken by patients or the public based on information provided by the SaMD

Below are some types of adverse incidents from using SaMD, with examples.

**Performance issues:** a technology remotely monitoring vital signs in a care home fails to correctly detect the assigned parameters (pulse rate, respiratory rate and oxygen saturation). This leads to a delay in diagnosis or treatment

**Diagnostic accuracy issue:** a dermatology app used for detecting melanoma gives an inaccurate result. As a consequence, the user decides not to seek an expert clinical opinion

**Decision support software resulting in harm:** a clinical calculator produces an incorrect calculation. A patient is prescribed the wrong amount of medication as a result

**Issues with connected hardware or software:** antivirus software installed on a device is non-compatible with the SaMD and causes it to malfunction (that is, the device that runs the software causes harm)

**User error resulting in harm:** a user enters the wrong value into a contraception app. The user relies on an incorrect output and unintentionally becomes pregnant

**Inadequate labelling and instructions for use:** a tablet-based SaMD is not labelled with the correct cleaning instructions, which leads to cross contamination between patients

**Computer system security problem:** a SaMD is the target of a cyber attack, causing corruption of patient data stored on the device. This leads to an incorrect or delayed diagnosis

Read the MHRA's guidance on reporting adverse incidents for Software as a Medical Device for more information, including examples of indirect harm and its causes.

 

You should notify the MHRA as soon as you become aware that your SaMD may have caused or contributed to a reportable incident. Report individual incidents on the MORE portal.

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 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 medical devices after deployment

### This is required guidance

It is legally required and it is 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 or medical devices that are already on the UK health and social care market, you will need to:

- assess how significant the changes are for each update, and
- consider whether you need to reapply for approval

# Monitoring changes to the intended purpose of your technology

After placing your digital technology on the market, you may want to add new functionality or improve aspects of your technology. For example, you may need to update your technology to meet new security requirements. Or, if the performance of your technology drops, you may want to change or update your technology to improve or bring performance back in line with acceptable or prespecified levels. This is required for medical devices.

For medical devices it is important to understand whether this new functionality changes the intended purpose of the technology. If it does, extra reviews before the approved body or competent authority allows the update will be required and a complete re-assessment against the regulations may be needed.

For non-medical devices, you will need to consider whether previous evaluations (for example, health economic modelling) are impacted by the change.

If your medical device changes, you will need to justify such a change.

You may have to go back to the beginning of the technology lifecycle to:

- make sure you gain relevant approvals
- meet appropriate standards for the updated technology
- generate the relevant evidence to make sure the technology is still operating legally
- generate the relevant evidence to make sure the technology is safe and effective for its new purpose

Plans for change management should be in place during the technology development stage.

 

# Determining significant changes to your digital technology

Updates to digital technologies are changes that happen after the technology has been placed on the market. These can be:

- minor (for example, removing bugs)
- significant, such as a software change that replaces previously required user input to a closed loop decision or change in use

For further detail on what constitutes a significant change see:

- Guidance for manufacturers and Notified Bodies on reporting of Design Changes and Changes of the Quality System
- Notified Body Operations Group

It is worth noting that technology changes may be done proactively or reactively. For example, a proactive change may involve updating a digital technology to improve user experience or resource usage based on customer feedback.

A reactive change may be based on a safety concern or change in cybersecurity requirements. Beyond determining whether a technology update is significant or substantial, you may need to consider how this relates to other aspects of post-market surveillance such as safety reporting.

# Requesting to make a significant change

You must assess proposed updates to medical devices before they are deployed. This will form part of the internal release processes and benefit risk analysis under your quality management system.

When you have planned significant changes, you cannot deploy the technology without getting them ratified by the approved body overseeing the technology. This process will be assessed during QMS audits. Failure to comply with requirements can lead to additional costs and potentially the removal of your technology from the market.

 

# Responses to safety concerns

In some cases, you will need to update a technology because of an identified or suspected safety concern. In this case, there are requirements under the UK Medical Devices Regulations (UK MDR 2002) under post-market surveillance to:

- assess incidents
- report them to the MHRA
- investigate the root cause, and
- address the issue

Within this process there are requirements to inform users of technology changes.

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.

 

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: 29 August 2025

Last updated: 29 August 2025

**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.

Creating statistically realistic synthetic data may require processing some real data first to establish model parameters. Where that real data relates to identified or identifiable individuals, its use must comply with data protection law. Read more here How should we assess security and data minimisation in AI? | ICO

Get more information on anonymisation:

ICO guidance on anonymisation

 

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: 29 August 2025

Last updated: 29 August 2025

**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

 

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: 29 August 2025

Last updated: 29 August 2025

**Reviewed by:** Health and Care IG Panel

- The ICO's guidance on AI and data protection
- The ICO 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

 

Category

# Cyber security and resilience

Cyber security and resilience

# Cyber security and resilience for digital healthcare technologies

### This is required guidance

It is legally required and it is an essential activity.

### This Guide covers:

- England

### From:

- Information Commissioner's Office (ICO)
- Department for Health and Social Care

Last updated: 18 April 2024

Cyber security is the protection of devices, services and networks and the information on them from theft or damage. It's essential for providing effective care, protecting patient and service user safety and maintaining trust in services.

**The Network and Information Systems Regulations**

The Network and Information Systems (NIS) Regulations 2018 place security and reporting duties on relevant digital service providers (RDSPs).

RDSPs are organisations that provide specific types of digital services:

- online search engines
- online marketplaces
- cloud computing services

To be an RDSP you must provide one or more of these services, have your head office in the UK or provide digital services within the UK (where your head office is outside of the UK, in which case you must nominate a representative in the UK).

Small and micro organisations are exempt. If you have fewer than 50 staff and an annual turnover or balance sheet below €10 million then you are not an RDSP, and the NIS Regulations do not apply. But if you are part of a larger group, you should assess the group's staffing and turnover numbers to see if the exemption applies.

RDSPs are required to register with the Information Commissioner's Office (ICO). This is the competent authority (regulator) for RDSPs. Under the NIS Regulations, the ICO has powers to:

- issue an information notice requiring an RDSP to provide information
- do an inspection after an incident
- issue an enforcement notice requiring action to address failings
- issue a penalty notice for a financial penalty up to £17 million

**Reporting incidents to the ICO**

Under the NIS Regulations, RDSPs are required to notify the ICO of any incident that has a substantial impact on the provision of their services. You must notify the ICO without undue delay and no later than 72 hours. You can assess whether you need to notify and report an incident using the ICO's incident reporting guide. You should also consider notifying the National Cyber Security Centre at the same time.

**Personal data breaches**

 

Under the UK General Data Protection Regulation, incidents that result in a personal data breach must be reported to the ICO. See how to comply with the UK GDPR for more information.

**Adverse incidents for medical devices**

If your technology is a medical device, you must report any adverse incidents to the Medicines and Healthcare products Regulatory Agency using its MORE portal. For more information, see post-market surveillance of medical devices and identifying adverse incidents for software as a medical device.

**Data Security and Protection Toolkit (DSPT)**

The DSPT is NHS England's online self-assessment tool for data security and protection requirements. If your organisation has access to NHS patient data and systems, you must use the toolkit to show you're practising good data security and that personal information is handled correctly.

Your organisation should complete and publish a DSPT assessment in accordance with the DAPB0086: Data Security and Protection Toolkit information standard published under section 250 of the Health and Social Care Act 2012.

**Cyber Essentials**

Cyber Essentials is a self-assessment certification that helps you protect your organisation against cyber attack. The government requires suppliers bidding for certain types of public contracts (for example those where personal data of citizens, such as home addresses, is handled by suppliers) to hold Cyber Essentials or Cyber Essentials Plus certification (or demonstrate that equivalent controls are in place). Organisations with Cyber Essentials Plus certification do not have to respond to some DSPT questions. But Cyber Essentials Plus certification is not required for completing the DSPT.

**The Cyber Assessment Framework**

The National Cyber Security Centre's Cyber Assessment Framework is a tool for assessing cyber resilience (the extent to which cyber risks to essential functions are being managed by your organisation). It is widely used across other sectors and will be rolled out for health and care as updates to the established DSPT process. The framework establishes cybersecurity outcomes without defining how they should be met, empowering your organisation to manage its risk proportionately and with autonomy. Further information on implementation timelines for your organisation will be published on the DSPT website.

**Digital Technology Assessment Criteria**

 

If you want your technology to be used in the NHS or social care, you may be asked to demonstrate that it meets the standards set by the Digital Technology Assessment Criteria (DTAC). These include cybersecurity requirements. During procurement, adopters will review your completed DTAC to make sure your technology meets minimum standards.

**Further reading**

- ICO: The Guide to NIS
- Cyber security strategy for health and social care: 2023 to 2030 on GOV.UK
- National Cyber Security Centre: advice and guidance

 