Adopters guidance

All adopters' guidance

Contents

Category

Identifying the problem

Identifying the problem

Understanding if digital technologies or AI are the right solution to a problem

This is best practice guidance

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

This Guide covers:

- United Kingdom

From:

- NHS England

Last reviewed: 23 January 2023

You need to assess whether digital healthcare technologies or AI are the right solution to the problem you are trying to solve. There may be a simpler solution.

Identifying the problem

Starting with the problem you are trying to solve should be the first step of any decision to use a digital or data-driven technology such as AI. You need to map the current care pathway, and use the NHS service standard to help you identify problems and understand end-user needs. This is particularly important for new technologies, whose novelty might make it easy to overlook this critical step. You might then consider, 'what is it about this technology that makes it a good choice for addressing this problem?'. Ask yourself what you are looking to improve in your service, and what metrics matter in measuring this improvement.

You should describe and quantify the quality improvements, savings and efficiencies that using AI would create for your organisation. If the technology may result in only small improvements, you might reconsider the need for it.

Deciding whether AI is the right solution for the problem

To help you decide whether AI is the right solution, see government guidance on assessing if AI is the right solution and a guide to good practice for the use of digital technology in health and social care. You will need to think about whether:

- there is enough data for an AI model to learn from, and whether you can test the technology on historical data in your organisation to evaluate its potential impact
- you can do a pilot study to test whether this impact can be achieved in a live, operational setting
- the data can be used ethically and safely in a secure data environment
- the outputs of the model could be tested for accuracy against a 'ground truth' (that is, information that is known to be real or true, provided by direct observation and measurement)
- the model outputs would lead to problem-solving that achieves outcomes in the real world
- a clear accountability framework could be set up to monitor ongoing safety and effectiveness, including how this varies across demographic groups

Thinking these considerations through may help you identify a simpler solution to the problem. It may also help you meet regulatory requirements if you choose to use AI, such as:

- legal and ethical use of data
- evidence of effectiveness and clinical benefit
- equalities considerations
- post-market surveillance

Category

Assessing the right technology to use

Assessing the right technology to use

Complying with NHS Digital clinical risk management standards

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- AI and Digital Regulations Service
- NHS England

Last reviewed: 12 January 2023

If you want to adopt a digital technology on behalf of 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. They help developers evidence the clinical safety of their technology. They assure adopters that the technology is safe to use in health and social care.

As an adopter, standard DCB0160 requires you to:

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

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

If the digital technology does not meet these standards, you should not adopt it.

How to meet NHS Digital standard DCB0160

As an adopter, you must:

- think about how the digital technology will be deployed and used
- make sure the developer is compliant with DCB0129
- do a clinical risk assessment
- provide evidence of effective risk management
- present your findings to the adopter

Use the relevant standard DCB0160 Clinical Risk Management: its application in the deployment and use 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.

As an adopter, you may wish to use the Digital Technology Assessment Criteria (DTAC) to support your procurement. 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.

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 integrating a medical device into your IT infrastructure you are recommended to use standard IS0 IEC 80001-1:2021 (Application of risk management for IT-networks incorporating medical devices — Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software). This supports the safe, secure and effective introduction of such devices.

Assessing the right technology to use

Understanding the evidence for a technology before adopting it

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)
- NHS England

Last reviewed: 31 October 2023

When deciding whether to adopt a digital healthcare technology, you need to review the evidence and make sure you understand it.

How to review evidence about a digital technology

Step 1: Checking whether NICE has evaluated the technology

NICE evaluates digital healthcare technologies that address areas of unmet need in health or social care. It reviews the evidence and publishes guidance and advice on these technologies. If NICE has evaluated a technology, this can help you decide whether to adopt it.

NICE guidance

NICE guidance summarises the clinical and cost effectiveness of a technology. It recommends whether the technology should be used in the NHS, and in some cases recommends how it should be used.

You can search NICE guidance and advice to check whether a technology has been evaluated.

Learn more about how NICE evaluates technologies in its health technology evaluations manual.

Early Value Assessment

Early Value Assessment (EVA) produces a faster assessment of a promising technology that is still developing its evidence base but has the potential to meet important needs in health or social care services. EVA recommends whether the technology should be used in the NHS while further evidence is generated.

EVA also outlines the gaps in the evidence base. This is used to develop an evidence generation plan, which NHS adopters can use to guide them in producing real world evidence.

Learn more about EVA and how it is done on NICE's Early Value Assessment webpage.

Step 2: Reviewing the evidence using NICE's evidence standards framework

Using NICE's evidence standards framework (ESF) can help you make informed and consistent decisions about adopting digital healthcare technologies.

Evaluating a digital healthcare technology can be challenging. Using the ESF helps you make decisions about whether to adopt a digital technology. It describes the types and levels of evidence the technology should demonstrate to be adopted by a health or social care service, including standards on security and data governance.

It is particularly important that you review the technology using the ESF if there is no NICE guidance for it. But it is prudent to use the ESF to review the technology even if there is NICE guidance, because:

- digital technologies can change, such as changes to the interface or new features, that might impact the effectiveness as it was originally assessed
- new evidence on clinical and cost effectiveness may have been produced after the guidance was published
- the ESF includes practical guidance for deployment, which will help you during the implementation phase

You can use the ESF to help decide whether to pilot an early version of a technology or include it in an innovation programme.

The ESF is designed for local or regional evaluations of a digital technology. It is intended to stand alongside the regulatory and other standards for digital technologies, not to replace them.

How do I use the ESF?

The ESF has 21 standards for 'mature' digital technologies (that is, technologies that have a robust evidence base on safety, clinical and cost effectiveness). These are grouped into 5 areas of the digital technology's life cycle: design factors, describing value, demonstrating performance, delivering value and deployment considerations.

There are different evidence standards based on the intended use of the technology, and these are grouped into tiers. You need to determine the evidence tier for the technology, then review the appropriate evidence standards.

You can use the ESF to help assess a technology that does not yet have a full evidence base to support its use. There are 16 ESF standards that help you do this.

To start using the ESF, go to NICE's evidence standards framework for digital health technologies.

Step 3: reviewing the technology against the Digital Technology Assessment Criteria

The NHS Digital Technology Assessment Criteria (DTAC) sets out specific standards for digital healthcare technologies. For a technology to be used in the NHS or social care, it needs to meet the required standards. It is important you understand the assessment criteria when considering whether the digital technology meets these required standards.

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.

There is alignment between the DTAC and the ESF, and you will see reference to many of the same standards and regulatory requirements in both. But they differ in focus; the ESF focuses on evidence of clinical and cost effectiveness, while the DTAC focuses on minimum requirements for use in the NHS.

So, it is important you use both the DTAC and the ESF when assessing a technology.

Reviewing the developer's DTAC responses

The developer should have completed the DTAC by responding to the questions and providing the evidence required. You need to review the developer's responses and assess whether the digital technology meets the required standards.

It is important that staff reviewing the DTAC have the relevant expertise to assess the digital technology; for example, the clinical safety section should be assessed by a qualified Clinical Safety Officer.

For more information on how developers complete the DTAC, see using the NHS Digital Technology Assessment Criteria.

Step 4: thinking about your public sector equalities duties

When you use a technology in providing care, you need to monitor its effectiveness. This includes its impact on different groups, such as the potential for data-driven technologies to produce biased results that worsen health inequalities. Technologies can also have a positive impact, such as improving experiences for groups who often have a negative experience of health or care services.

Public sector organisations have specific equalities duties that are important to consider when using AI and digital technologies in health and social care.

Before you adopt a technology, you need to think about how using it might impact equalities. Read our guide on the public sector equalities duties to help you think about the monitoring you'd need to put in place if you choose to use an AI or data-driven technology. This can help you make a more informed decision when choosing whether to adopt it.

Assessing the right technology to use

Thinking about whether a medical device will meet your needs

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 updated: 07 June 2023

You need to think about whether the medical device is fit for purpose and likely to meet your needs before deciding whether to adopt it.

Getting information about the device

You can ask the developer to provide information that helps you decide whether the device is right for you. The developer should have documents describing the device's functionality, limitations and risks. These will have helped it show compliance with the UK Medical Device Regulations 2002 (UK MDR 2002). The developer does not have to share these documents with you. But if it is open and transparent with this information, you may have greater trust in the developer and the device.

Understanding the intended purpose

You should make sure you understand the 'intended purpose' of the device; that is, what exactly it can be used for and the exact conditions under which it can be used. The developer should have written an intended purpose statement for the device. You can ask the developer for a copy of the statement. Sometimes you can find it in the regulatory certification documents or the instructions for use.

Understanding the intended purpose helps you decide whether the device is the right solution to a problem you are trying to solve. Be aware that using the device beyond its regulated intended purpose may have liability implications for your organisation and staff.

Understanding the medical device risk class

The developer should have used its intended purpose statement to help determine the medical device's risk class. These are Class 1, Class 2a, Class 2b or Class 3 (the higher the number, the higher the risk to patients).

A higher-risk device may have stricter controls on its use than a lower-risk device. If you are concerned that the risk class for the device is too low for its intended purpose or there is not enough evidence of safety, you can report this to the Medicines and Healthcare products Regulatory Agency (MHRA). See reporting safety issues about medical devices to the MHRA for more information.

Understanding UKCA and CE marks

The UK Conformity Assessment (UKCA) mark shows the device meets the requirements of the UK MDR 2002. It helps you know the device is safe, performs as intended and that the benefits outweigh the risks.

To get the UKCA mark, the developer will have gone through a conformity assessment. The developer does this assessment itself for lowest risk (class 1) devices. Higher-risk devices are assessed by an approved body. There are several approved bodies in the UK and the developer should have chosen a suitable one to assess the specific type of medical device.

A developer based in Great Britain should have obtained the UKCA mark before placing the medical device on the market. This is a legal requirement. But developers in the European Union go through a similar process and get a European conformity (CE) mark. A CE mark for medical devices is currently recognised in Great Britain, so the device you are considering may have this instead of a UKCA mark. But there are limitations on recognition of CE marks based on the risk class and the specific legislation that applies to the device. If the device you are considering has a CE mark, not a UKCA mark, check our what's new page regularly for updates.

Checking MHRA registration

To place a medical device on the market the developer (or their UK Responsible Person) and the device must both be registered with the MHRA. You can check this on the MHRA's Public Access Registration Database.

Further reading

See the MHRA's guidance on regulating medical devices in the UK and implementation of medical devices future regime.

Category

Planning for implementation

Planning for implementation

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 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 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.

Planning for implementation

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

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: 13 January 2023

The Ionising Radiation (Medical Exposure) Regulations (IR(MER) 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

Planning for implementation

Planning for local validation and integrating a digital 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)

Last reviewed: 13 January 2023

It is important to integrate and validate digital healthcare technologies before deploying them in a health or care service. Adopters should plan for this during procurement, in liaison with the developer or vendor.

Understanding local validation and integration

Local validation is the activities you do to check a digital healthcare technology will achieve its required performance levels in your health or care service. Digital technologies cannot usually be deployed directly 'off the shelf'; that is, you need to take your local environment and IT set-up into account. This is a particular consideration for AI and data-driven technology because of dependency on the data it was trained on and how it generalises to your local population. Local validation activities include calibration and longer-term pilot studies. It may take time to fully understand whether the device is performing as it should in your service.

What you need to do before integrating a digital technology

Developers should deliver their healthcare technologies to you with defined performance levels of safety. This is a requirement of the UK Medical Device Regulations 2002. But the technology may not perform perfectly in your specific environment (depending on your infrastructure, culture, work force and local population). Before 'going live' (deploying) a technology, you typically need to agree activities with the developer to integrate and validate it.

Local validation activities to make sure performance levels are reached include:

- testing the device using local data sets to make sure processing can occur and within expected performance levels. If possible, assess device performance against specific sub-populations within your local population to check the technology generalises to your needs
- stress testing against your local requirements. This is to make sure the device can function within the expected workflow to meet clinical timelines, and to check for performance issues in the local patient population
- calibrating device parameters to maximise local performance. Note that performance must not drop below safe levels

- doing longitudinal studies or silent-mode testing to explore performance across a wider population sample and understand the impact of drift on performance

Planning for implementation

Piloting digital technologies in a health or care service

This is best practice guidance

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

This Guide covers:

- England

From:

- National Institute for Health and Care Excellence (NICE)

Last reviewed: 11 October 2024

Before deciding whether to adopt a digital healthcare technology, you may need to pilot it in your service.

Understanding local piloting

Before adopting a digital healthcare technology, you should have evidence showing its clinical and cost effectiveness in a setting like yours. If evidence relevant to your context is limited, the developer should have plans to generate it. Testing the technology in your service (local piloting) may be part of this plan.

You might do a pilot study for other reasons, including to:

- learn about potential risks or technical and implementation issues associated with the technology in a controlled way before 'going live' (deploying) it
- understand how the technology affects current care or operational workflows, and whether this creates risks or issues that need to be managed
- learn how to use the technology most effectively and adjust processes to get the best value from it
- plan processes for monitoring the technology after it is deployed

Piloting gives stakeholders confidence that the technology creates benefits in your setting, and that any decision to adopt it is well-evidenced.

Planning a pilot study

Your pilot study should have:

- a defined scope
- a data-collection plan
- clear criteria for success or failure
- a defined time period (start and finish dates)
- defined roles and responsibilities for you and the developer so that both your interests are met appropriately

The pilot study should generate results that help you decide whether to continue using the technology. So, your data-collection plan should define what and how much data

to collect and how it will be analysed. This will allow you to assess the benefits of the technology. Types of data you might collect include:

- healthcare professionals' experiences of using the technology
- experiences of patients or service users
- clinical or care outcomes
- cost effectiveness
- efficiency gains or losses
- operational or financial impacts on your service

Resources to help you design a pilot study

Resources that may help you design a pilot study include:

- NICE's real-world evidence framework. This provides general guidance on planning, doing and reporting real-world evidence studies. This will help because you'll be doing the pilot study in a real-world setting, using data collected routinely in your service
- The DECIDE-AI reporting guidelines, which aim to improve reporting of studies
- NICE's evidence standards framework for digital health technologies. This provides standards on evidence requirements for different types of digital healthcare technologies (which it refers to as DHTs). See the table below for evidence standards that are particularly relevant for thinking through different stages of pilot development

Relevant NICE evidence standards for developing a pilot

Planning a pilot study

Make sure the value proposition for how the technology will fit into local clinical pathways and its expected benefits are clear:

- Standard 10: describe the intended purpose and target population
- Standard 11: describe the current pathway or system process

- Standard 12: describe the proposed pathway or system process using the DHT
- Standard 13: describe the expected health, cost and resource impacts compared with current care or system processes

Planning for deployment

Make sure the technology deployment plan for the pilot provides relevant information about deployment requirements:

- Standard 19: ensure transparency about requirements for deployment
- Standard 20: describe strategies for communication, consent and training processes to allow the DHT to be understood by end users

Clinical or care outcomes

Identify the data collection requirements to demonstrate the relevant outcomes:

- Standard 14: provide evidence of the DHT's effectiveness to support its claimed benefits
- Standard 15: show real-world evidence that the claimed benefits can be realised in practice

Experiences of patients or service users

Identify the data collection requirements to demonstrate the relevant outcomes:

- Standard 14: provide evidence of the DHT's effectiveness to support its claimed benefits
- Standard 15: show real-world evidence that the claimed benefits can be realised in practice

Experiences of health care professionals

Identify the data collection requirements to demonstrate the relevant outcomes:

- Standard 14: provide evidence of the DHT's effectiveness to support its claimed benefits
- Standard 15: show real-world evidence that the claimed benefits can be realised in practice

Efficiency gains or losses and their operational or financial impact on your service

Identify the data collection requirements to demonstrate the value of the technology:

- Standard 17: provide a budget impact analysis
- Standard 18: for DHTs with higher financial risk, provide a cost-effectiveness analysis

Planning for implementation

General staff training and product-specific user training for digital healthcare technologies

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)
- NHS England

Last reviewed: 04 December 2023

There are 2 levels of training adopters need to consider for digital healthcare technologies: general training for all staff so they understand how to implement, use and govern technologies and product-specific user training so they can use specific technologies.

General staff training in digital healthcare technologies

General user training should be part of broader education and training for all staff about digital healthcare technologies. This includes foundational training in digital technology principles and advanced training for specific roles and responsibilities.

Health Education England has researched the different knowledge, skills and capabilities required for different NHS staff groups to be confident using AI. A lot of these would also apply to other digital healthcare technologies. Read the HEE's report on understanding healthcare workers' confidence in AI (part 1) for more information. HEE has also proposed AI-related learning and skills for specific staff roles in the health and social care system. It's report on developing healthcare workers' confidence in AI (part 2) will help you understand what training and upskilling you might need yourself or to provide for others in your organisation.

HEE also delivers Digital, Artificial Intelligence and Robotics Technologies in Education (DART-Ed). This explores the educational needs of health and care workers. It can help you understand the impact of digital healthcare technologies on education and training needs.

Product-specific user training for digital healthcare technologies

Without product-specific user training, you might face challenges implementing new digital technologies and the safety and performance of your service could be at risk. This is particularly relevant to technologies classified as medical devices.

For medical devices, there is not a direct legal requirement for training under UK Medical Device Regulations (2002). But if the developer determines that training of intended users is required for the device to meet safety requirements, you are legally required to do this under health and safety legislation on training and competence.

For further information on training requirements for medical devices, see the MHRA's guidance on managing medical devices.

Why is product-specific user training important?

Product-specific user training is the training needed to use a specific digital healthcare technology safely and effectively.

Lack of understanding of new digital technologies, and lack of appropriate confidence in using them, can be barriers to successful implementation. This can lead to wasted resources, workflow inefficiencies and substandard patient care. It could lead to disparities in who gets to benefit from digital technologies, which may be unethical.

What product-specific user training is needed when integrating a technology?

The aim of product-specific training for users is to help them use the technology to its maximum potential. This includes making clinical decisions with appropriate confidence and awareness of the abilities and limitations of the technology.

The training is usually based on information provided by the developer. But you may need to tailor it to the users and clinical setting in which the technology is being deployed.

Developing product-specific user training involves:

Understanding the clinical context and users' experience levels

You need to think about:

- how the technology will be used, who by and with what degree of human oversight
- whether the users will be clinical experts
- whether users have experience using other digital healthcare technologies in similar or different contexts
- how the level of clinical and service risk affects users' confidence in decision making

Designing training

When designing the training, you need to:

- agree training requirements and required information in collaboration with the developer (or vendor) to develop knowledge and appropriate confidence in using the technology
- consider the social factors that could affect implementation including users' attitudes and concerns, resistance and workarounds, expectations, benefits, values and motivations
- engage with users and ask for their input in design, training, support, identification of champions and integration with existing work practices
- select existing resources or develop new resources with the developer to inform your training materials
- consider how to provide product-specific information for patients in clear English, so they understand the digital technology and how it might affect them
- consider how to educate staff to communicate with patients, so they can help them understand the digital technology and inform them about its risks and benefits

Delivering training

Consider options for:

- in-person or virtual delivery of the training
- internal or external support for queries and further information

Evaluating training

Evaluate users' knowledge and confidence using the technology clinically, using tools such as:

- surveys
- written feedback

Example: one type of training and information you may require is understanding the characteristics of the technology and how it will be integrated

The developer should provide you with the characteristics of the digital technology. You need to consider how the technology will be integrated into the clinical workflow. Your considerations will be specific to the technology, but could include:

- the intended purpose and scope of use
- information about training and validation datasets including their size, demographics and impact on fairness and confidence
- information on potential biases and algorithmic errors that require risk management, including information on performance for subgroups in the target population
- details of explainability and transparency features and their intended use, if appropriate
- processes required for recording errors and reporting adverse incidents

Category

Using the technology

Using the technology

Understanding 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: 13 January 2023

Post-market surveillance of medical devices is the legal responsibility of the developer. But it is important for adopters to understand and support post-market surveillance of medical devices.

Adopters' role in supporting post-market surveillance of medical devices

As an adopter, you play a role in making sure a medical device is safe to use. This includes understanding how the developer does post-market surveillance for the device, so you can support it.

When developers place medical devices on the UK market, they have a legal requirement to:

- collect and analyse data on the performance and safety of the device
- have a system in place to do this
- report safety issues to the MHRA and investigate the root cause

This 'post-market surveillance' makes sure an adopted device is acceptably safe to use for as long as it is in use. You play an essential role in supporting this (for example, helping the developer understand how the device is performing). You should also report safety concerns about medical devices directly to the MHRA using the Yellow Card reporting site.

How adopters support post-market surveillance

You and the developer should agree a plan for ongoing data collection about the performance and safety of the device. You will consider together what data the developer needs and how this should be collected and distributed. You should also discuss and agree on how quickly these activities can occur; developers will be required to meet timelines set by regulations. For example, does the developer need actual clinical outcomes to assess the clinical performance of the device? If so, you will need to consider data regulations for digital technologies and allocate staff time.

Your organisation should have a clearly identified person responsible for collecting and providing the required data to the developer.

For more information about ongoing data collection, see NICE's Evidence Standards Framework. The Evidence Standards Framework is designed to support local or regional evaluations of a digital technology.

Using the technology

Monitoring the safety and effectiveness of digital technologies (real-world monitoring)

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

It is important to monitor digital technologies used in health or care. This is because their safety and effectiveness can reduce over time, leading to poor outcomes for patients or service users.

Why monitoring is important

AI and data-driven technologies contain algorithmic systems and models. These models may be affected by changes in the external environment, which can result in changes to product performance, outside of previously validated safety and value criteria. An AI specific example of this is drift, in which the model's performance and accuracy decays (reduces) over time.

There are 2 main types of drift:

- Data drift - the input data differs from the data originally used to train the model. For example, demographic data for the local patient population can change because of an increase in age or arrival of new ethnic groups
- Concept drift - the relationship between the target variable and the input features changes.

For example, a technology developed to diagnose Covid-19 from symptoms can drift when new variants arise with a different set of symptoms

Note that internal processes in a model also cause drift, even if there are no changes in the external environment.

The performance of the technology may reduce because of drift. This can result in poorer or harmful outcomes for patients and service users. It may also increase the risk of algorithmic bias, meaning some groups of individuals are more affected than others. So, you should continuously monitor the technology to detect model drift.

Your responsibilities as an adopter

The developer has a legal responsibility to maintain the safety of medical devices. This includes doing 'post-market surveillance'. You have a responsibility to help the developer do this. For more information see post-market surveillance of medical devices.

Whilst the legal responsibility to identify, report and address post market medical device failures falls upon the developer as outlined above; there is a direct route for users and adopters of medical devices (including software and AI) to report

concerns. We encourage anyone with concerns or direct evidence of failures to report this to the MHRA via our Yellow Card reporting system.

The developer may want to make updates to the model or introduce new features to the technology. You have a responsibility to assess the impact of these changes. You should work with the developer to make sure the changes are safe and effective. See managing change to medical devices after adoption for more information. If you are in England or Wales such monitoring is legally required by the standard DCB0160.

Technologies that are no longer supported by developers (legacy systems) have higher risk of reduced performance. They require careful monitoring and management. See managing legacy systems for more information.

Your monitoring processes may identify concerns about the safety and effectiveness of the technology. You should report such concerns through your internal risk-management processes, directly to the developer and to the MHRA's Yellow Card system.

What happens if you do not do continuous monitoring?

Reduced technology performance can result in harm to patients. For example, if a condition is diagnosed incorrectly the wrong treatment may be prescribed.

Drift can result in unwanted biases in the algorithmic processing. These biases accumulate over time. If you do not have due diligence in monitoring and mitigating such bias, there may be discriminatory outcomes for patients.

Note that liability has not been established for harmful outcomes related to healthcare technologies. So, you should not assume that full liability will fall on the developer. Your organisation may face reputational damage and legal action for breaches of the Equality Act 2010.

Using the technology

Reporting safety issues about medical devices to the MHRA

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: 13 January 2023

Adopters should report safety concerns about medical devices to the MHRA via the Yellow Card reporting site.

How adopters report safety issues to the MHRA

You should report a suspected safety issue ('adverse incident') with a medical device to the MHRA as soon as possible. How to report it depends on where you are in Great Britain:

- England and Wales - use the Yellow Card reporting site
- Scotland - report it to Health Facilities Scotland (unless you are a private facility providing care to private clients, in which case report to the Yellow Card reporting site and the Care Inspectorate)

You should also notify the developer of the technology.

Please note that reporting medical device concerns in Northern Ireland currently falls under the EU Medical Device Regulations. For more information please contact the MHRA .

Understanding the criteria for reporting adverse incidents

An adverse incident is an event that caused, or almost caused, an injury to a patient or other person, or a wrong or delayed diagnosis and treatment of a patient.

Developers have a legal requirement to report incidents to the MHRA.

The MHRA encourages adopters to follow the same criteria as developers to determine if something is an adverse incident. An event that meets all 3 criteria below is considered an adverse incident and you should report it to the MHRA:

- an event has occurred. This includes situations where testing performed on the device, examination of the information supplied with the device, or any scientific information indicates some factor that could lead, or has led, to an event
- the device is suspected to be a contributory cause of the incident
- the event resulted, or might have resulted, in death or a serious deterioration in state of health of a patient, user or other person

Not all adverse incidents result in death or a serious deterioration in health. These may have been prevented because of other circumstances, or because of intervention. An event is still reportable if no injury was sustained but could be upon a repeat event. So, you should still send the MHRA a report if:

- an incident associated with a device happened, and
- if it occurred again, it might lead to death or serious deterioration in health

The MHRA, the developer or a medical specialist may investigate the problem depending on how serious it is. It'll be recorded to help prevent similar incidents in future, even if it's not investigated.

Using the technology

Managing changes to medical devices after adoption

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: 13 January 2023

Managing changes to medical devices is the legal responsibility of the developer. But adopters support developers in these processes and are required to follow the clinical risk management standard. These help make sure devices stay safe and effective.

Changes to medical devices after you adopt them

Medical devices may change after you adopt them. There are 2 types of changes you need to consider:

- change to the device driven by the developer
- changes to the infrastructure and procedures of the deployed environment, driven by you as the adopter

Reasons for changes include:

- safety concerns
- updates to operating systems
- security patches
- user feedback
- design improvements
- testing out new features
- using the device in a new area of working

If performance drops for a medical device, the developer is required to update it and bring performance back in line with acceptable or prespecified levels. Developers may also want to add new functionality or improve other aspects of their devices.

Some changes (for example, new functions or changes in intended purpose) may require developers to go back to the beginning of the device life cycle and seek approval. They will have to generate the relevant evidence, meet appropriate standards for the updated device, make sure it is still operating legally and is safe and effective for its new purpose. They may also be required to consider whether previous evaluations (such as health economic modelling) are adversely impacted by the change and need re-evaluating.

Adopter's responsibilities when a device changes

If you are an adopter only (that is, not involved in developing the device) you have no legal requirements under medical device legislation (UK MDR 2002) if a medical device changes after you adopt it. But the developer has legal requirements to maintain device safety and may need your help to meet them. Also, if you are in England and Wales, you are required to comply with clinical risk management standard DCB0160. For example, as part of your general monitoring of the device, you may need to consider whether re-evaluations of the clinical safety of the device are necessary when there is a significant change in it or the external operating environment.

You can work collaboratively with the developer to put in place agreements and processes for managing change without losing use of the device. You should also establish appropriate risk management and safety monitoring as required by DCB0160 and make users aware of these processes.

You will be routinely providing the developer with information and data about outcomes and performance to help inform device improvements and updates. This will have been agreed as part of the post-market strategy. You may need to provide more information and data after a major change (or safety investigation) to enable further assessment by the developer.

You need to be aware that any infrastructure or operational changes within your own working environment could impact the function of the device. These include changes in the target population or recommended use. You should inform the developer of any changes. If there is a change in use, the developer may need to apply for new approvals.

You need to be aware that any infrastructure or operational changes within your own working environment could impact the function of the device. These include changes in the target population or recommended use. You should inform the developer of any changes. If there is a change in use, the developer may need to apply for new approvals.

An example: changes to infrastructure

You adopted a medical device into your infrastructure and this infrastructure has a scheduled update of its operating system. The developer is legally required to make sure the device continues to perform within safe parameters after this update has been implemented. They need to test and adjust the device in a controlled manner before it can be deployed in the updated infrastructure. By planning the update in advance with

the developer you avoid technical delays, drops in performance and potential safety issues.

Addressing concerns or incidents after changes to a medical device

If users experience any difficulties or concerns about the usability or outcomes after a change to the system that could impact the clinical safety of the updated device, you should report these. For example, if there is a clinical safety concern such as a pattern of incorrect diagnosis you would use the safety incident management process agreed in your DCB0160 report. You should also report your concerns to the developer and support them in their investigation and resultant updates. You should also report any concerns or adverse incidents after device updates to the MHRA using the Yellow Card reporting site.

An example: a poorly-performing device has resulted in an injury

A person has been injured as a result of a poorly-performing device. The developer is legally required to report this to the MHRA, who may require the developer to investigate the root cause of the event and take corrective action. The developer needs access to the specific inputs and outputs from the event. If this involves sharing personal data, you will need to follow legal requirements. The developer then needs to update the device and there are risks from using the device until the update is available. Working collaboratively with the developer, you make sure effective solutions are generated quickly and within regulatory requirements.

Your role as an adopter in managing change to a digital technology

Your role in making sure a medical device is safe to use includes understanding how the developer does post-market surveillance. This is the legal responsibility of the developer, but you play an important role in supporting it. For more information, see understanding post-market surveillance of medical devices

If you, as an adopter, are also the developer of the medical device you should read our website content on developer obligations.

Get more information on clinical risk management standard DCB0160 here.

Using the technology

Meeting your public sector equality duties

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- Wales
- England
- Scotland

From:

- Equality and Human Rights Commission (EHRC)

Last reviewed: 06 February 2023

Public bodies should consider the public sector equality duty when thinking about whether to use digital healthcare technologies. This also applies to any digital healthcare technologies that public bodies are already using or that others are developing or using on their behalf.

Understanding the public sector equality duty

The public sector equality duty (the equality duty) was created under the Equality Act 2010. It covers the 9 protected characteristics: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, marriage and civil partnership, sex and sexual orientation.

Using digital technologies may lead to discrimination and deepen inequalities in health or social care. This is because of inherent biases in the training and development of digital technologies, including the data used to train them. Biases can accumulate over time as a technology is used. You should monitor for discriminatory outcomes to make sure you are able to identify and tackle any bias or unintended impacts on people with one or more protected characteristics.

For an overview of the equality duty see the guides for public authorities in England, Scotland and Wales from the Equality and Human Rights Commission (EHRC). Note that equality is an 'ongoing duty'. You should regularly monitor and evaluate digital technologies to make sure they are working as intended and not causing any unlawful discrimination.

The equality duty has 2 parts:

- **the general duty** applies to public authorities and organisations carrying out public functions
- **specific duties** apply only to public authorities named (or listed) in specific duties regulations

Meeting your general equality duties

The general equality duty requires public authorities and organisations to have due regard to the need to:

- eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by the Act

- advance equality of opportunity between people who share a protected characteristic and those who do not
- foster good relations between people who share a protected characteristic and those who do not

Meeting your specific equality duties

The specific equality duties relevant to digital healthcare technologies are likely to be those relating to:

- assessing equality impact (this applies in Scotland and Wales only)
- procurement and commissioning (this applies in Scotland and Wales only)
- setting equality objectives and publishing information to show compliance with the general duty (and with equality outcomes in Scotland)

Workforce-related obligations are also likely to be relevant if you are using digital healthcare technologies in your employment.

Doing an equality impact assessment is not a legal requirement in England but is good practice. Public bodies, if challenged, should be able to evidence how they have considered the potential equality implications of the digital healthcare technologies they are using or proposing to use. Doing a risk assessment is a legal requirement in England to meet the safety standard DCB0160, and this could include an assessment for bias.

Useful resources

See the EHRC's guide to artificial intelligence in public services, which includes a checklist for public bodies in England and non-devolved and cross-border public bodies. It explains how to comply with the equality duty if you do not have a specific duty to do an equality impact assessment.

See the NHS Race and Health Observatory for resources to identify and tackle health inequalities experienced by Black and ethnic minority communities in England.

Note that inappropriate use of digital healthcare technologies may lead to breaches of laws such as the Data Protection Act 2018 and the Human Rights Act 1998.

Using the technology

Planning for managing legacy systems and decommissioning digital healthcare technologies

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: 13 January 2023

It is important to plan for managing legacy systems and decommissioning before deploying a digital healthcare technology. Adopters should do this planning during procurement, in liaison with the developer or vendor.

What are legacy systems?

A legacy system is an outdated or unsupported technology that is still in use. It relates to digital technologies that are one or more of the following:

- considered an end-of-life technology
- out of support from the supplier
- impossible to update
- no longer cost effective
- considered above the acceptable risk threshold

Managing legacy systems

There are risks inherent in retaining legacy systems, for example:

- the digital technology may become less reliable
- it may be difficult to know what data is held within the technology and how to migrate it

If the technology is no longer supported by the developer, the post-market surveillance function will stop. So, the technology will not be updated to solve bugs or respond to any changes in input data and target population. This will affect its ongoing performance and reliability and potentially impact negatively on patients or service users. This is a particular consideration for data-driven technologies because of the potential for drift, so performance does not stay the same over time. Retaining an unsupported technology can expose systems to other vulnerabilities including cyber attacks. Once there is no identified developer, adopters may be taking on the liabilities for the use of the digital technology.

The management of legacy systems depends on your organisations overarching IT strategy. However, there may be a point when you need to decommission a digital technology and manage migration to newer technologies.

Decommissioning a digital healthcare technology

Digital technologies may need decommissioning because of increased risks associated with a legacy system, or because of organisational or system changes.

Decommissioning a digital technology carries risks that need to be considered and addressed before the decommissioning happens. Digital technologies may hold data that will need to be extracted into a secure environment or securely migrated to a newer system. The process of decommissioning may cost time and money, and needs appropriate staffing to manage the process. So, the decision to decommission needs to consider whether the risks associated with retaining a legacy system outweigh the risks of decommissioning and migrating data.

Planning ahead during procurement

During procurement, you need to agree considerations and processes for the end-of-date of the digital technology (if known) and decommissioning. The developer should provide the information you need. If you are in England and Wales your organisation will assess this information using section 7.4 of standard DCB0160, specifically:

- considering the requirement for a clinical risk management process for technology decommissioning
- taking into account the succeeding technology
- addressing migration of data, and
- issuing a clinical safety case report to support decommissioning

The UK government's guidance on managing legacy systems has 7 key principles for you to consider:

- Aim to use continuous improvement planning to keep your technology up to date
- Build a complete and accurate register of your data assets
- Know the full extent of your systems and infrastructure
- Build the skills and capabilities of your IT team
- Have a flexible and responsive service model which can adapt to changing technology
- Consider the organisation's business needs, processes and culture

- Use the Technology Code of Practice as a basis for your decisions

For more information on each principle and the processes to consider, see the government's guidance on managing legacy systems.

You may need to consider other standards and processes when addressing data migration issues. For more information on data migration, see the data management guide for adopters.

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 for adopters

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

When integrating, piloting or deploying new digital healthcare technologies, adopters need to process health and social care data. You need to know what legal requirements govern the use of this data and when to get research approval. For the purpose of this guide, adopters are considered to be users of the technology, who may work in:

- social care
- NHS organisations (providers and commissioners, including primary care, community care and mental health)
- independent healthcare providers

Please note: a longer and more technical version of parts 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.

See ICO's website for comprehensive general guidance on UK data protection law.

For guidance on information governance (IG) in the health and care sector in general, see the NHS Transformation Directorate's 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 by adopting 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 adoption 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 the adopted technology's lifecycle
- how to implement a data protection 'by design and by default' approach
- how and when to do a data protection impact assessment (DPIA), and how it will benefit you and the patients or 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)
- 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** is information, both clinical and demographic (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 recognises the importance of maintaining trust in health and care services, so that all individuals can be reassured in fully engaging with these service 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 original data no longer apply to those receiving it in modified form

Get more information about 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: 13 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 the adopted technology's lifecycle

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Education England (HEE)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

When considering adopting digital healthcare technologies, you need to know that data protection legal requirements will apply at the following stages:

Before buying a digital technology

You need to understand what to expect from developers and the key issues to think about, before buying a technology. You should consider whether the technology is compatible with your existing systems and infrastructure

Integration and piloting

When integrating or piloting a technology, including doing compatibility testing, you need to consider compliance with data protection legislation. It imposes requirements to make sure personal data is processed lawfully, fairly, and transparently

Post-rollout

Once you have rolled out the technology, you will have to monitor it for safety and efficacy. There will be ongoing data-related requirements related to this, which may involve further research, service evaluation or be part of direct care.

Direct care is also known as individual care. People in the individual care team are health and care staff who the individual would reasonably expect to have access to their record for individual care.

Care teams may include doctors, nurses, and a wide range of staff on regulated professional registers, including social care professionals. The most important thing is that a member of a direct care team has a legitimate care relationship with the specific patient or service-user individual whose data they access. So, this excludes entrepreneurs not working within NHS or social care organisations in England and Wales.

Considerations before buying a digital technology

Before buying a digital healthcare technology, you should check the developer has complied with the relevant regulations. For example, the developer needs to have registered with ICO, nominated a data protection officer, and completed a Data Security and Protection Toolkit and a Data Protection Impact Assessments (DPIA).

You should try to understand the developer's approach to make sure you understand their approach to complying with the law and regulation, including its choice of legal basis allowing it to provide you with access to personal data and/or confidential patient and service-user information. See the developer pathway guide for detailed information on what laws and regulations developers need to consider. Further reading:

- Digital Technology Assessment Criteria from the NHS Transformation Directorate
- Guidance on Digital and data-driven health and care technology from the Department of Health and Social Care
- Data protection by design and default from ICO
- Toolkit for organisations considering using data analytics from ICO

Regulations that govern the use of data

Data considerations related to compatibility testing

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

Both developers and adopters must make sure that use of data during compatibility testing is done lawfully.

Compatibility testing may involve the use of patient and service-user data that may not be for direct care or does not constitute a research activity. You should use the HRA's decision tool 'Is my study research?' to assess whether a project has characteristics indicative of a research activity requiring regulatory approval.

You need to think about data protection and confidentiality, for example:

- Is the use of personal and/or confidential patient and service-user information necessary, or could your purpose be achieved in other ways?
- Who is accessing confidential patient and service-user information and 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 compatibility testing

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

If health and care data need to be processed, and even if the processing does not constitute research, data protection law will still apply. While processing anonymous data falls outside data protection law, data controllers should carefully consider the risks from reidentification and data matching (matching data to a person) as part of determining whether anonymisation standards have been met. When considering whether anonymisation is effective, you should review ICO's guidance on anonymisation

Confidential patient and service-user information processed by someone within the direct care team

If confidential patient or service-user information (collected in direct-care provision) needs to be processed to carry out testing, you should consider whether those holding such information have a legal basis to share such data with those that would do the testing. When such information does not need to be shared with people outside the direct care team for testing, no further action is needed.

Confidential patient and service-user information processed by someone outside the direct care team

If confidential patient or service-user information is shared with someone outside of the direct care team for testing purposes, either explicit consent to such sharing must be obtained from the individual, or (where not possible or highly impractical to get consent in the situation), 'section 251 support' must be obtained. You will need to apply to the Confidentiality Advisory Group (CAG) via the HRA and HCRW to set aside the common law duty of confidentiality to permit the sharing where the activity is deemed research, or direct to CAG via the Secretary of State where not (that is, in non-research cases). An example would be when manual work with confidential 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.

Read getting research approvals for more information on applications to CAG.

Regulations that govern the use of data

Technology adoption: using 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: 13 January 2023

Reviewed by: Health and Care IG Panel

You may need to use health and care data during the adoption of the technology. Often this cannot be anonymous data because that would be inappropriate for achieving the clinical or care 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 (see step 4 of complying with the UK GDPR). The disclosure of any **confidential patient and service-user information** to you as an adopter (when you do not work as part of the direct care team) will also need to have a lawful basis under the common law duty of confidentiality. **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
- the common law duty of confidentiality (for both living and deceased individuals)

Regulations that govern the use of data

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

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

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

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

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

Regulations that govern the use of data

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

Step 1: Register with ICO

This is required guidance

It is legally required and it is an essential activity.

From:

- Health Research Authority (HRA)

This Guide covers:

- England

Reviewed by: Health and Care IG Panel

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

How to do it:

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

Regulations that govern the use of data

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

Step 2: Consider doing a DPIA

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

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

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

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

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

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

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

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

Regulations that govern the use of data

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

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

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

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

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

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

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

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

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

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

Decision tool:

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

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

Regulations that govern the use of data

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

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

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Overseen by: HRA (Health Research Authority)

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

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

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

Article 6 of the UK GDPR

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

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

Get more information:

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

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

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

Article 9 of the UK GDPR

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

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

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

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

Get more information:

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

Regulations that govern the use of data

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

Step 5: Determine if your activities are research

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

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

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

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

More information:

- HRA Approval
- ICO's guidance on research provisions

Do you need research approval?

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

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

What approvals do I need?

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

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

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

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

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

How to apply for research approvals

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

Being transparent with research

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

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

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

HRA's best practice in public involvement

Regulations that govern the use of data

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

Step 6: medical device clinical investigation approval

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

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

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

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

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

Step A: Notify the MHRA

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

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

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

Step B: Submit a REC application

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

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

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

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

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

Regulations that govern the use of data

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

Step 7: Follow the 8 Caldicott Principles

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Health Research Authority (HRA)

Last reviewed: 13 January 2023

Reviewed by: Health and Care IG Panel

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

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

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

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

Get more information:

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

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: 15 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 an individual 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, 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

See guidance from the NHS Transformation Directorate on consent and confidential patient information for more detail.

You should also consult your organisation's information governance team for advice.

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

Data access and re-identification risk intervention

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

If you share, or provide access to, health and care data with the developers of a digital technology, you will need to consider the identifiability of the data. Adopters should not provide personal data unless strictly necessary to achieve a particular lawful purpose (with a lawful basis).

Any arrangement should be covered by a data sharing agreement, or a controller-processor contract, which will need to be prepared and signed by you and the developer.

If you are proposing to share confidential patient or service-user information outside your health or care setting, you should first make sure you have a lawful basis in place to share such information under the common law duty of confidentiality. Unauthorised access would constitute a breach.

How to process anonymous data

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

Usually, you do not need consent or approval to process data that has been rendered anonymous before you have received it. This is because, when a person cannot be identified from data, its use is not subject to the common law duty of confidentiality or data protection legislation.

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 on ICO's website. You should check ICO's website from time to time as new guidance becomes available.

In this process of anonymising personal data, an organisation must modify 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 third-party using means (reasonably likely available to them) to re-identify the individual, and thus to make sure it meets effective anonymisation requirements. A key benefit of this is that is 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 of complying with the UK GDPR). A lawful basis under the common law duty of confidentiality is required to disclose confidential patient or service-user information with someone who would then apply anonymisation processes to the data. Where the anonymisation is to be

performed by someone who does not have a legitimate relationship, there will be a disclosure, 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 the 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: 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 ICO's 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 but a type of safeguard. 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 or processing contract and other appropriate safeguards to prevent re-identification by the recipient. The determining factor is whether the recipient can use the modified data (on its own, or in conjunction with other available data using

reasonable means) to identify an individual. You need to consider the processes necessary to make sure data is rendered anonymous or effectively anonymous. See ICO's guidance on anonymisation

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

Regulations that govern the use of data

Understanding the difference between research and non-research activities

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: 15 January 2023

Reviewed by: Health and Care IG Panel

It can be difficult to decide whether an activity is research or not. You might intend the activity to be service evaluation, service improvement, service development or audit. The main distinctions are:

- research is designed to generate generalisable or transferable new knowledge (that is, produce results to be extrapolated or applied to a different setting). That may or may not involve new interventions. Treatment allocation using randomisation may only be done in research
- service evaluation is designed to answer the question 'what standard does this service achieve?'. It only involves interventions that are well established within a service. Choice of treatment is decided between the patient and clinician. Service improvement or development seeks to find out what improvements could be made to the quality of a service
- audits are designed to find out whether the quality of the service meets a defined standard

To help you assess whether an activity is considered research, use the HRA's decision tool 'Is my study research?'

You should pay particular attention to your underlying intentions in carrying out the activity and remember that intentions can change over time. What started as service evaluation may later become a research activity, for example, which may require approvals.

Regulations that govern the use of data

Data Protection agreements and contracts

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

Reviewed by: Health and Care IG Panel

It is important for adopters to have appropriate data agreements and contracts in place to formalise arrangements around access to and use of health and care data.

Below are the 2 types of agreements and contracts you should consider:

A Data Sharing Agreement

A Data Sharing Agreement (DSA) is a written agreement put in place to govern the sharing of personal data between 2 or more independent data controllers. It is good practice to have a DSA because it sets out the purposes for data arrangements, covers what is to happen to the data at each stage, sets standards, and helps all the parties to be clear about their respective roles. It can help your organisation demonstrate compliance with data protection law.

You can use the standardised data sharing and processing agreement template developed by the Health and Care IG Panel. If the research uses data received direct from NHS organisations, you should use one of the HRA's templates for supporting documents available on IRAS to complete the DSA.

A Controller–Processor Contract

If a controller uses a processor to carry out a particular processing activity on personal data it controls, a written contract (agreement) must be in place. As mentioned previously, controllers are the main decision-makers. Processors must meet the controller's standards defining the purposes and means of the processing of personal data.

You can use the standardised data sharing and processing agreement template developed by the Health and Care IG Panel. When NHS organisations will be the processors, you should use one of the HRA's templates for supporting documents available on IRAS.

The UK GDPR sets out what needs to be included in the contract. This is summarised in ICO's guidance on contracts, which highlights necessary considerations so that both parties understand their responsibilities. For example, if a processor uses another organisation (that is, a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor.

Regulations that govern the use of data

Using data during deployment and after rollout

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: 15 January 2023

Reviewed by: Health and Care IG Panel

Deploying your adopted digital technology: using health and care data

Direct care encompasses the processing of health and care data in the delivery of care to an individual (such as in the adoption of a healthcare technology used directly in treatment of a patient). However, direct care does not encompass pre- or post-deployment testing or adoption of the 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 measurement of outcomes done by one or 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 satisfy an Article 6 legal basis and an 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 individual or direct care

Information: 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

Changing a technology's purpose

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: 15 January 2023

Reviewed by: Health and Care IG Panel

If you, as the adopter, use data in a different way than originally intended, you need to consider whether this has changed the intended purpose of processing for the technology. For more information, see managing change.

A change in processing purpose has implications for your obligations under data protection law.

You should also consider whether this changes your activities into research and whether approvals will now be required.

Updates affecting research with REC, HRA or CAG approval

If your research project that has already been approved subsequently changes to involve collection of new or different patient data, you will have to create an amendment.

Amendments are changes made to a research project after approval from a review body has been given. If you plan to make an amendment to your research project, you will need to determine whether you need to notify the review bodies from whom you have received approvals.

You should notify the HRA and REC by submitting the amendment through IRAS. If the research involves a medical device your submission should include the MHRA. If the project has s.251 support (to set aside the common law duty of confidentiality) you will also need to notify CAG.

For more, see:

HRA's guidance on amending an approvals

The amendments help section in the Integrated Research Application System (IRAS)

Important notes on repurposing data:

- if you want to 'repurpose' data collected for one purpose for a new purpose, this is known as 'secondary processing'. UK GDPR requires you to have a new lawful basis in place before you do this. 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

- 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. You will need to make sure you have a new lawful basis before 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. Find information on how to assess compatibility in 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
- 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 for a purpose not covered by the original consent, to make sure your new processing is fair and lawful. You should also update your privacy information to make sure your processing is still transparent

Get more information:

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

Category

Cyber security and resilience

Cyber security and resilience

Cyber security and resilience for health or care services

This is required guidance

It is legally required and it is an essential activity.

This Guide covers:

- England

From:

- Medicines and Healthcare products Regulatory Agency (MHRA)
- 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 your service.

The Network and Information Systems Regulations

The Network and Information Systems Regulations 2018 aim to improve cyber security. Network and information systems (NIS) include:

- electronic communications networks
- devices or groups of interconnected devices that automatically process digital data, and
- digital data stored, processed, retrieved or transmitted by either of the above for the purposes of their operation, use, protection and maintenance

The regulations place security and reporting duties on an operator of essential services (OES). Healthcare services are an essential service under the regulations. The OESs in England are:

- NHS trusts or foundation trusts
- integrated care boards
- certain independent providers of healthcare

The regulations require an OES to:

- take appropriate and proportionate technical and operational measures to
- manage risks posed to the security of the NIS on which its essential service relies
- minimise the impact of incidents affecting the security of the NIS used for the provision of its essential services
- report any incident that has an adverse effect on the security of the NIS and a significant impact on the continuity of the essential service, within 72 hours. Your organisation should do this using the Data Security and Protection Toolkit (DSPT)

These duties also apply where there are physical and environmental causes such as interruptions to power supply or flooding.

Enforcing the NIS Regulations

The Secretary of State for Health and Social Care is the competent authority (regulator) acting through the Department of Health and Social Care. They are responsible for overseeing the NIS Regulations for healthcare services in England.

Under the NIS Regulations, the Secretary of State for Health and Social Care has powers to:

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

Data Security and Protection Toolkit

The DSPT is NHS England's online self-assessment tool for data security and protection requirements. It includes the NIS Regulations. 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. It helps you guard against the most common cyber threats and demonstrates your commitment to cyber security.

You may use Cyber Essentials to meet contractual obligations with other organisations, such as insurance providers or suppliers. Some contracts require Cyber Essentials or a higher level of certification (Cyber Essentials Plus). 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 government also 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).

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

The Digital Technology Assessment Criteria (DTAC) include cybersecurity requirements for digital technologies used in health or social care. You can assess a developer's completed DTAC during procurement or as part of a due diligence process, to make sure the digital technology meets minimum cybersecurity standards.

Medical devices

Digital healthcare technologies classified as medical devices are regulated by the Medicines and Healthcare products Regulatory Agency (MHRA). It has published a plan to address cybersecurity issues for medical devices - see it's cyber secure medical devices work package for more information.

You should report safety concerns about medical devices to the MHRA using its Yellow Card scheme or via the Yellow Card app.

Further reading

- The Network and Information Systems Regulations: guide for the health sector in England on GOV.UK
- Cyber security strategy for health and social care: 2023 to 2030 on GOV.UK
- National Cyber Security Centre: advice and guidance

