GOV.UK

Guidance

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

Updated 14 January 2021

Contents

Print this page

This publication is available at https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology

Introduction

Across the country and around the globe, digital innovators are helping us deliver our commitment to the digital transformation of health and social care, to bring benefits to patients, the workforce and the system as a whole. NHS England's Long Term Plan sets the direction towards widespread digitally-enabled care. The Secretary of State's Technology Vision goes on to articulate a clear ambition for the generation of more digital services designed around user need and adhering to key principles of privacy, security, interoperability and inclusion.

It is our duty as NHS England and central government to capitalise on these opportunities responsibly. The healthcare system is a unique space where a variety of regulatory ecosystems overlap. Due to the privileged nature of dealing with people's health and their protected data, the system is covered by various pieces of legislation as well as professional and ethical standards. Innovators in this field may come from sectors that are not necessarily familiar with medical ethics and research regulation, and may utilise data sets or processing methods that sit outside existing NHS safeguards.

At the same time, the wider NHS – patients, professionals, commissioners, purchasers – need a means of obtaining assurance and confidence across these domains so they can fulfil their duty to provide the best care to patients and the best value to the system.

What we have in the UK is a thriving digital innovation sector. We also have a receptive market in the form of the health service. However, we hear from both sides about the challenges of getting an innovative product into active service.

This guide is designed to support innovators in understanding what the NHS is looking for when it buys digital and data-driven technology for use in health and care, so that these principles of good practice can be built into the strategy and product development 'by design'. This, in turn, will mean that when products are presented for assessment or procurement, many of the criteria in the specification will have already been met. The intention is to smooth the path between development and procurement so that the NHS may realise the benefits that digital technologies can bring.

This guide is an update to the 'Code of Conduct for Data-Driven Health and Care Technologies'. We hear from innovators that they valued the practical advice within the Code and this has been strengthened and expanded upon in this update. The principles relating to data in the original Code have been grouped under Principle 6 and 7 in this document. Guidance on technical assurance, clinical safety, and regulation have been expanded and now comprise their own chapters. The document has been updated throughout to reflect the latest position, for example, in light of Brexit and the creation of the Centre for Improving Data Collaboration. Links have also been checked and updated.

1. How to operate ethically

Review the Data Ethics Framework and abide by the principles

Rationale

While digital and data-driven health and care technologies will have the potential to deliver significant benefit patients, clinicians, carers, service users and the system as a whole, we must approach the adoption of these promising technologies responsibly and in a way that is conducive to public trust. The NHS's reputation for delivering safe and ethical care must be upheld as we seek to innovate.

Furthermore, increasing use of data-driven technologies, including artificial intelligence (AI), could cause unintended harm if we do not think about issues such as transparency, accountability, safety, efficacy, explicability, fairness, equity and bias. For example, there is a risk that it could benefit some groups at the expense of others.

People need to know that their data is being used for their benefit and that their privacy and rights are safeguarded. Innovators are responsible for ensuring people are properly informed about how and when data about them is shared so that they may feel reassured that their data is being used for legally, fairly and equitably.

The Data Ethics Framework (https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework) is designed to inform and enable the development and adoption of safe, ethical and effective digital and data-driven health and care technologies. It clearly sets out the behaviours we expect from those developing, deploying and using data-driven technologies, to ensure that everyone abides by the ethical principles for data (https://www.nuffieldbioethics.org/publications/biological-and-health-data) initiatives developed by the Nuffield Council on Bioethics. Page 9 of the Guide to the Report contains useful definitions of the 4 principles below:

- respect for persons
- respect for human rights
- participation
- accounting for decision

2. Have a clear value proposition

Ensure that the product is designed to achieve a clear outcome for users or the system

Rationale

Every good product starts with a clear answer to the questions ‘what problem are you solving? For whom? How?’. It is imperative that digital health products and services have a clear purpose. Suppliers and potential suppliers should understand how their innovation or technology will result in better provision and/or outcomes for people and the health and care system. This could be through:

- improvements in patient outcomes or experience
- generation of new knowledge and capabilities
- generation of a firmer evidence base, and reduction in uncertainty
- efficiency improvements

This section is about making sure you can articulate the proposed value of the product and how you use this as the starting point for gathering evidence to back up any claims (covered further under later sections e.g. Usability, Effectiveness etc. We have found that companies that can do this well have identified clear product market fit and are much more compelling and hence more likely to be successful.

When summarising the value proposition, consideration should be given to:

- the problem or need that exists
- how the proposed solution meets the need

- how the solution will fit in with existing or new healthcare structures
- how the effectiveness of the solution is evidenced
- the cost-effectiveness of the solution
- capacity to scale
- how the solution will be sustainable over time

Understanding user needs

One of the best practical ways of getting to a clear value proposition is to research and define user needs thoroughly, and then involve users as much as possible in the whole life cycle of the product, through discovery, design, change and post-release review. Understanding the people and their specific needs will help with uptake and adoption of the technology or innovation being built, as well as clearly showing a commissioner or buyer the problem being solved.

In health and care, users can be patients, family, carers, staff or any combination of those roles working together to achieve an outcome. They may well have existing capacities and ways of solving their problem, which innovation might sustain or disrupt. Health and care services are for everyone, including people with different physical, mental health, social, cultural or learning needs.

If you are unsure how to carry out good user research, advice can be found in the Government Digital Service manual on user research (https://www.gov.uk/service-manual/user-research) and the NHS Digital design service manual (https://www.nhs.uk/transformation/manual/digital-service-standard.html).

Defining the outcome and how to prove it

The next step is to consider the generation of key performance indicators or other outcome measures that will be used to evidence success and identify potential improvements. It is wise to consider these as early as possible. It is a common mistake to leave it to the end, but it affects the entire development plan for the product. Outcomes or impact could be considered through 3 lenses:

- clinical/scientific outcomes
- impact on patient experience
- impact on workforce or workflows
- value for money, financial impact

Where possible, outcomes and KPIs should be published alongside assessment methodology and linked back to user need. Point 1 (https://www.gov.uk/service-manual/service-standard/point-1-understand-user-needs) and 10 (https://www.gov.uk/service-manual/service-standard/point-10-define-success-publish-performance-data) of the Government Digital Service Standard relate to articulating a value proposition.

3. Usability and accessibility

Ensure that the product is easy to use and accessible to all users

Rationale

Usability is central to the successful implementation of any technology, and health technology is no exception. Conversely, poor usability is a key source of frustration and can lead to failure of adoption. Common popular consumer products are often cited as examples where usability has been designed so well as to be entirely intuitive.

We expect suppliers to be able to demonstrate how they have designed and evaluated their product with users during every stage of the life cycle. We appreciate that companies will employ different methods to conduct relevant user research.

Tools such as a System usability scale (https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html) can be a quick and useful way of capturing feedback. Other suppliers may follow ISO standards related to usability, for example:

- ISO 9241 - 210: 2019 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems (https://www.iso.org/standard/77520.html)
- ISO 62366-1:2015 Application of usability engineering to medical devices (https://www.iso.org/standard/63179.html)

If the product is a self-management tool or supports a healthcare intervention, innovators should be able to demonstrate that relevant clinical expertise has been involved in the design, testing and sign off of the product even if the predominant end user will be patients or the public.

Accessibility

Health and care services are for everyone, including people with different physical, mental health, social, cultural or learning needs. Health technology designers should consider the needs of a diverse set of users to ensure the product is accessible to as many people as possible (https://www.gov.uk/service-manual/helping-people-to-use-your-service/understanding-wcag). Furthermore, the NHS is committed to improving health inequalities, and not making them worse. In the healthcare space, it matters that products are not solely for the digitally literate as this could disadvantage important groups of people. Design must consider the digital literacy of the nation and particular patient cohorts to ensure it is inclusive. Development teams should also consider the impact of accessibility on other domains such as clinical safety.

The caveat to this is that it is recognised that in some instances, in designing to maximise accessibility, we may miss serving the majority well. In such cases, innovators or their customers should give careful consideration to the use of assisted digital approaches. More detail can be found in the Government Digital Service's Government approach to assisted digital (https://www.gov.uk/government/publications/government-approach-to-assisted-digital/government-approach-to-assisted-digital).

Internet-first policy

Since 2013, the NHS has had an NHS Internet First policy (https://digital.nhs.uk/services/internet-first/policy). The ambition is that all new health and social care digital services should be made internet-facing from day one and that existing services should be upgraded to meet these standards as soon as possible. The policy is applicable to all health and social care digital services that present or expose services to end users or integrating systems outside of an internal network.

Making digital services available over the public internet supports the requirements for health and social care professionals to work flexibly from a variety of locations, using a range of access methods. This will reduce complexity and cost for many organisations, particularly for small health and social care providers, and reduce reliance on the centrally provisioned private networks required to support many applications and systems today.

4. Technical assurance

Ensure that the product is appropriately tested and is fit for purpose

Rationale

It is important that there is a structured approach to software development that involves control of testing and improvement cycles. International standard IEC 62304 is a standard which specifies life cycle requirements for the development of medical software and software within medical devices. All health technology should be sufficiently tested across a range of domains as appropriate and listed below, to evidence that it is suitable for its stated purpose and will provide a robust and stable service.

It is good practice to set out an assurance plan that describes the approach to testing and explains how the data-driven technology will continue to be developed and managed. This would normally include how users will continue to be involved and what resources are in place to test and monitor it for technical faults during its lifetime and when a new version is released. However, what's most important is that appropriate testing is carried out, recorded and results acted up to assure quality prior to release.

Types of testing include:

- validation testing – that the design of the product serves the intended purpose. This can include end-user testing and acceptance
- verification testing (functional correctness): checking that the requirements of the product have been appropriately implemented
- load testing: that it performs reliably under continued stress and load
- performance: that it maintains responsiveness under various loading conditions
- regression testing: to prove that the product still performs as expected following a change or update
- security, for example penetration testing
- integration testing
- unit and system testing
- bias testing/monitoring

The solution should be provided with appropriate Service Level Agreements, or equivalent, regarding ongoing technical support with suitable availability from a helpdesk or similar.

Digital health technologies for use in health and care should usually have the ability to roll back to a previous version, should any significant problems be encountered following an update. An appropriate Disaster Recovery and Business Continuity Plan should be in place. This should be explicit in covering how any risk to patient data and, more importantly, patient health, will be limited and mitigated.

5. Clinical safety

Ensure that the product is clinically safe to use

Rationale

All digital health technologies must be clinically safe to use. The development process for data-driven software for clinical purposes contains key differences to the development of software for general purposes. These should be well understood and factored into operations from discovery.

The development of clinical products benefits from technical expertise sitting side by side with clinical expertise in the form of a Clinical Product Owner. This avoids the common pitfall of having to attempt to retrofit necessary clinical input on quality and safety too late in the development process.

To sell into the NHS, manufacturers must demonstrate compliance with the Clinical Safety Standards (https://digital.nhs.uk/services/clinical-safety/clinical-risk-management-standards) referred to as DCB0129 (http://content.digital.nhs.uk/isce/publication/scci0129) and DCB0160 (https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0160-clinical-risk-management-its-application-in-the-deployment-and-use-of-health-it-systems). This is mandated under the Health and Social Care Act 2012.

DCB0129 requires manufacturers to:

- have a clinical safety management system - a defined process by which clinical safety is considered during design, pre-release and in response to any information about incidents
- carry out specific clinical risk management activities, usually in the form of a ‘hazard workshop’ - a systematic approach to the identification of risk and mitigating actions
- to maintain the following related clinical safety documentation:
    - a hazard log for the product - effectively a clinical risk register for the product. It is a live document and should be kept up to date in the light of product changes or clinical incidents
    - a clinical safety case report. Prior to release, the safety case report should summarise hazards, their mitigation and the justification for release. This is a companion document to the hazard log
    - a clinical safety management plan - the document that describes how the clinical risk management system will apply to a particular product over the product life cycle

Evidence for hazard control often comes from the technical testing carried out on the product prior to release.

Suppliers should give a copy of their DCB0129 hazard log and clinical safety case report to customers so they can carry out their duty of compliance with DCB0160, the companion standard. The customer will carry out a similar structured risk assessment considering the product in the circumstances of their own specific deployment.

It is a requirement that all documents are approved by a Clinical Safety Officer (CSO). A CSO is a clinically-qualified individual who has undergone appropriate specific training with NHS Digital. This person should ideally be involved in the clinical risk management activities and verify that appropriate processes have been followed.

If the product requires clinicians to operate it, organisations must supply details of clinicians involved and their relevant professional registration.

In addition, evidence must be shown of origin and provenance of clinical reference sources.

6. Data protection

Demonstrate that the product collects, stores and processes users' information in a safe, fair and lawful way

Use data in line with the law and appropriate relevant guidelines

Be aware that as well as the legislation surrounding the handling of personal information, there are also specific rules that apply to handling confidential patient information.

Legality: Innovators must comply with the law. They are responsible for not only ensuring their innovation complies with relevant legislation such as GDPR/Data Protection Act 2018 but also demonstrating this. They should also ensure the legal basis for processing confidential patient information.

Justifiability: Innovators should be able to explain to a member of the public why the data that was used was needed and how it is meeting the user need.

Proportionality: Explain the necessity and proportionality of the data (https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en). This applies to both data use in the research or testing period and after the digital health product goes live and is used as part of standard care. Wherever possible it is preferable to use anonymised data in testing rather than identifiable patient data. The following question series can be helpful in determining if data processing is necessary and proportionate:

- is it necessary to collect/use personal information?
- is it necessary to process it in this particular way?
- could you use anonymised data instead?
- are you collecting/processing more data than you really need?
- do the advantages of processing this data outweigh any disadvantages?
- does processing this data allow you to achieve the envisaged objective?
- could you use other less intrusive means to achieve the same objective?

The Caldicott Principles (https://www.ukcgc.uk/manual/principles) are the 7 fundamental principles that govern the use of confidential patient information and everyone dealing with or looking to use patient information should be familiar with them and comply with them. Chapter 4 of the report 'Artificial Intelligence: how to get it right' (https://www.nhsx.nhs.uk/media/documents/NHSX_AI_report.pdf) contains more information specific to artificial intelligence products.

If using patient data or accessing NHS patients in order to conduct healthcare research to either develop a proof of concept or test a digital health tool (sometimes referred to as health technology assessment), conform to the UK Policy Framework for Health and Social Care Research (https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/uk-policy-framework-health-social-care-research/). Approval should be sought from an Ethics Committee to access patient data.

Patient data may be accessed either for research or for clinical investigation. Access for research purposes is used for the generation of research papers. When using a device for research only, it is not considered to have a medical purpose as it is not intended for clinical use. This also means that devices in this situation are considered to be excluded from medical device regulations. As such, they only

require local ethics approval through the trust, clinical commissioning group (CCG) or research institution. However, the results form research and this cannot be used to provide clinical evidence for CE marking.

Patient data accessed for the generation of clinical evidence for CE marking requires a clinical investigation registered with the Medicines and Healthcare products Regulatory Agency (MHRA) through the Integrated Research Application System (https://www.myresearchproject.org.uk/) (IRAS). Ethics approval is sought through the Health Research Authority (HRA) and provided by a Research Ethics Committee. Devices should be labelled 'exclusively for clinical investigations'. All clinical investigations should comply with ISO 14155.

Access to confidential patient information requires explicit patient consent, or where this is impracticable, approval under section 251 of the NHS Act 2006. For further information, see the HRA information on data-driven technology (https://www.hra.nhs.uk/datadriventech).

Information that has been anonymised so that it cannot be used to identify a person either directly or indirectly is no longer subject to the common law duty of confidentiality. The ICO's code of practice on anonymisation (https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf) (which is currently under review) and the UK Anonymisation Network's Decision-Making Framework (https://ukanon.net/framework/) provide guidance on a number of anonymisation techniques that may assist data controllers in anonymising personal data. However, it must be borne in mind that under the Data Protection Act 2018, the standard for anonymisation is high and data may still be considered personal data even if direct identifiers have been stripped out. Therefore, even after following the steps in the ICO code, data controllers will need to undertake a 'reasonably likely' test to ensure any data they disclose does not relate to identifiable individuals.

Since May 2018 the national data opt-out (https://digital.nhs.uk/services/national-data-opt-out-programme/supporting-patients-information-and-resources) allows people to opt out of their confidential patient information being used for purposes beyond their individual care and treatment. By 31 March 2021, any health and care organisation that processes and/or disseminates data that originates with the health and adult social care system in England is required to be in compliance with the national data opt-out policy. Data anonymised in line with the ICO's code of practice is exempt from this. Data flow maps will enable data controllers to be clear when the national data opt-out should be applied, as this is defined using the legal basis. The ICO have recently published top 10 tips for innovators (https://ico.org.uk/media/about-the-ico/documents/2618204/ih-report-20200828.pdf) regarding data protection compliance.

In some instances, building an AI model may require the persistence of data regarding individuals who do not have a particular disease as well as those who do have it, in order to learn about the process of the development of the disease. In cases such as these, the drivers, requirements and benefits of the data that is needed should be set out and justified in an application for data.

7. Data transparency

Be fair, transparent and accountable about what data is being used

The NHS has a number of safeguards in place to assure patients that their data is managed safely and securely and their rights to privacy and confidentiality are upheld. These requirements are particularly strict when processing health data, which is considered special category data (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-

processing/special-category-data/) under the Data Protection Act 2018. Other legal requirements (for example, the common law duty of confidentiality, Article 8 of the Human Rights Act 1998) and the Caldicott principles also need to be complied with if dealing with confidential patient data.

The Data Protection Act 2018 (https://www.gov.uk/data-protection) replaced the Data Protection Act 1998, introducing new obligations that require integration of data protection concerns into every aspect of processing activities. This approach is known as 'data protection by design and by default'. From a practical perspective, the important documents underpinning this are data flow maps, data protection impact assessments (DPIA) and privacy notices.

A good data flow map (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/) identifies the data assets (data at rest) and data flows (exchanges of data) that enable the relevant objective or initiative to be delivered. Where data flow mapping identifies instances where data is processed by a data processor on behalf of a data controller, a legally binding written data processing contract is required. This should include clauses appropriate to the processing risks identified (highlighted in the DPIA), as well as mandatory clauses for all data processing contracts.

The data flow map will then influence the DPIA (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) as the vehicle by which proposed flows of personal identifiable data are governed, and the controls developed to ensure lawful processing. The vast majority of data processing in a health and social care context will involve special categories of data and it is therefore almost certainly a requirement that a full DPIA is carried out. A DPIA is intended to be a 'living document' and should be regularly reviewed and updated by programmes. If a risk is identified that cannot be mitigated, the ICO must be consulted before processing commences. They will normally provide advice within 8 weeks, or 14 weeks in complex cases.

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the Data Protection Act 2018. A privacy notice, which should be made readily available to individuals, must provide details about who the data controller is and contact details for its data protection officer. It should also explain the purposes for which personal data is collected and used, how the data is used and disclosed, how long it is kept and the controller's legal basis for processing.

Data sharing agreements or contracts (https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf) are only valid between data controllers and are strongly recommended. They set out specific concerns relating to the data to be shared, as identified through data flow mapping and DPIA exercises.

Be transparent about the limitations of the data used

The data used must be well understood and reviewed for accuracy and completeness. Accuracy is the closeness of agreement between a data value and its true value. Completeness is the presence of the necessary data. NHS Digital publishes a quarterly data quality and maturity index (https://digital.nhs.uk/data-and-information/data-tools-and-services/data-services/data-quality), which provides data submitters with transparent information.

A 2-stage approach is suggested when applying analytics to any data. Algorithms should be trained to understand the levels of data quality first and then achieve their objective by using the variables given. This 2-stage approach should be built in so that high fluxes in data quality are handled appropriately.

Assessment of data quality should not be a one-off check – continuous anomaly detection should be in place to provide alerts to changes in a data source. NHS England (https://www.england.nhs.uk/publication/data-quality-guidance-for-providers-and-commissioners/) and the UK Statistics Authority (https://www.statisticsauthority.gov.uk/) have produced guidance on data quality, which should be referred to. Be aware of potential biases in the data used for training algorithms – consider the representativeness of the database used for training the algorithm. If the data provided for the AI to learn is limited to certain demographic categories or disease areas, this could potentially limit the applicability of the AI in practice as its ability to accurately predict could be different in other ethnic groups.

Good data linkage will avoid reducing data quality

There is a range of approaches for linking data, which can provide differing levels of accuracy and data loss. It is often necessary to strike a balance between good matching accuracy and loss of too many records. Consideration should be given to the effects of a selected linkage procedure on data quality. In particular, if the process could cause systematic loss or mismatching of a particular type of record, this could have downstream implications in model assumptions and algorithm training.

Linking datasets may require those carrying out the linkage procedure to use identifiable data to match the data. It is therefore important to ensure that anyone with access to the identifiable data has a legal right of access. Similarly, the process of converting an identifiable dataset into an anonymised one, if conducted by a person, will need to be carried out by someone with a correct legal basis. Where you can access data sets:

- Public Health England currently collects a range of data, made available in different formats, for example their fingertips tool (https://fingertips.phe.org.uk/), although plans for the future of this information following recent changes to PHE are not yet clear
- the Office for National Statistics collects a range of health-related microdata at their ONS virtual microdata lab (https://www.ukdataservice.ac.uk/media/604377/stirling_2016_05_12.pdf)
- Health Data Research UK (https://www.hdruk.ac.uk/research/) are in the process of building further training datasets
- Health Data Finder (https://www.nihr.ac.uk/researchers/collaborations-services-and-support-for-your-research/find-services-or-support/access-data-patient-cohorts-samples-support.htm)
- NHS Digital Data Access Request Service (https://digital.nhs.uk/services/data-access-request-service-dars)

Access must be requested for data that is not already in the public domain. The process for this varies depending on the organisation providing the data, and this should be detailed on the organisation's website. NHS Digital holds the responsibility for standardising, collecting and publishing data and information (https://digital.nhs.uk/data-and-information) from across the health and social care system in England. Whatever the details of the individual processes, most will require evidence of the data use being in the public interest or for public benefit.

Training versus deployment

Be clear on the strengths and limitations of the training versus deployment data set. If the algorithm has been built on a training set and not yet deployed in a real-world clinical implementation, transparency should be shown to that effect. Demonstrate whether the algorithm is published in a real-world deployed environment or a training environment.

Show what type of algorithm is being developed or deployed, the ethical examination of how the data is used, how its performance will be validated and how it will be integrated into health and care provision in compliance with data protection requirements around automated decision making.

Consider how the introduction of AI will change relationships in health and care provision, and the implications of these changes for responsibility and liability. Use current best practice on how to explain algorithms (https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/explaining-decisions-made-with-ai/) to those taking actions based on their outputs.

When building an algorithm, be it a stand-alone product or integrated within a system, show it clearly and be transparent of the learning methodology (if any) that the algorithm is using. Undertake ethical examination of data use specific to this use-case. Achieving transparency of algorithms that have a higher potential for harm or unintended decision-making, can ensure the rights of the data subject as set out in the Data Protection Act 2018 are met (https://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/3), to build trust in users and enable better adoption and uptake.

Work collaboratively with partners, specify the context for the algorithm, specify potential alternative contexts and be transparent on whether the model is based on active, supervised or unsupervised learning. Show in a clear and transparent specification:

- the functionality of the algorithm
- the strengths and limitations of the algorithm (as far as they are known)
- its learning methodology
- whether it is ready for deployment or still in training
- how the decision has been made on the acceptable use of the algorithm in the context it is being used (for example, is there a committee, evidence or equivalent that has contributed to this decision?)
- the potential resource implications

This specification and transparency in development will build trust in incorporating machine-led decision-making into clinical care.

8. Cybersecurity

Make security integral to the design and ensure that the product meets industry best practice security standards

Rationale

A core element of at-scale adoption and uptake is to ensure that security and data protection methodology have been incorporated. The Data Security and Protection Toolkit (https://www.dsptoolkit.nhs.uk/) replaces the previous Information Governance Toolkit to ensure that patient information is kept safe. All organisations that have access to NHS patient data and systems – including NHS trusts, primary care and social care providers, and commercial third parties – must complete the toolkit to provide assurance that they are practising good data security and that personal information is handled appropriately. NHS Digital's Data security and information governance resource list (https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance) also contains a number of documents that are relevant to helping secure medical devices.

The Department for Digital, Culture, Media and Sport has published a code of practice for consumer 'internet of things' (IoT) security (https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security), which sets out practical steps that will help manufacturers to improve the security of consumer IoT products and services and ensure products are secure by design. It is applicable to consumer IoT generally and is not specifically targeted towards health devices and systems.

The National Data Guardian's 10 data security standards are in place and form part of the NHS Standard Contract that goes out to all providers. The standards are set out in full in the National Data Guardian's Review of data security, consent and opt-outs (https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs). Completing the data security and protection toolkit (DSPT) is a means of evidencing that these 10 standards have been met.

When developing an application, ensure the product meets the OWASP Application Security Verification Standard (https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project), which is used to establish a level of confidence in the security of web applications.

The National Cyber Security Centre (https://www.ncsc.gov.uk/section/advice-guidance/all-topics) has more advice and guidance.

9. Regulation

Ensure that the product meets all relevant regulatory requirements

Establish if the data-driven technology that is being developed falls under the definition of a medical device (https://www.gov.uk/guidance/medical-devices-how-to-comply-with-the-legal-requirements) or in vitro diagnostic tool and follow the required regulatory conformance route required to place the product on the market (currently CE marking, soon to change to UKCA). Software that meets the definition of a medical device (https://www.gov.uk/government/publications/medical-devices-software-applications-apps) will be regulated as such by the MHRA (https://www.gov.uk/government/organisations/medicines-and-healthcare-products-regulatory-agency)). The Care Quality Commission (https://www.cqc.org.uk/guidance-providers/registration/what-registration) (CQC) regulates providers of clinical services, defined by 14 regulated activities (https://www.cqc.org.uk/guidance-providers/registration/regulated-activities). Any organisation using their products in a way that constitutes carrying out any of these regulated activities must register with CQC. Organisations using products involved in the delivery of pharmacy services should register with the General Pharmaceutical Council (https://www.pharmacyregulation.org/) (GPhC).

At present, it is the manufacturer's responsibility to determine which legislation applies to them. It is recommended that innovators spend time in the discovery phase working out whether the intended use of the intended product would fall within the scope of these regulations. The regulations themselves contain the necessary information for self-determination. If help is needed, specialist advice and guidance can be sought either from the competent authority (MHRA) or experts in the field. It can become complex if a product performs actions that fall under multiple regulatory bodies. The current process for managing this is to discuss the best way forward directly with the regulatory bodies.

Medical devices and in vitro diagnostics

The MHRA classifies medical devices as either Class 1, Class 2a, Class 2b or 3 in ascending order of perceived risk, as defined by the product's intended use statement. Class 1 products can apply a CE mark following self-certification whereas products classed 2a or above must undergo external audit from a notified body (https://www.gov.uk/government/publications/notified-bodies-for-medical-devices/notified-bodies-for-medical-devices).

If a product is classed as an in vitro diagnostic then it must also be registered with the MHRA and have a CE mark. In vitro diagnostics are classified as A, B, C or D in order of increasing risk, as defined by the product's intended use statement. Products in classes B, C or D require independent audit by a notified body.

Impact of leaving the European Union

During the UK's time as a member of the European Union, companies seeking to put their medical device on the market in the UK have been required to obtain a CE mark. This has been achieved by demonstrating conformity with the requirements in the EU Medical Devices Directive (MDD).

The competent authority, the MHRA, is currently reviewing the UK's approach to medical devices and in vitro diagnostics in light of the country's exit from the European Union. Government guidance published on 1 September (https://www.gov.uk/guidance/regulating-medical-devices-from-1-january-2021) details that the UK plans to replace the EU-controlled CE-Marking process with a UK-controlled procedure known as the UKCA (UK Conformity Assessed). The UKCA is a new UK product marking that will be used for certain goods, including medical devices, being placed on the Great Britain market after the transition period. Manufacturers will be able to use the UKCA mark from 1 January 2021.The UKCA mark will not be recognised in the EU, EEA or Northern Ireland markets, and products currently requiring a CE marking will still need a CE mark for sale in these markets. UK notified bodies will no longer be recognised in EU law and will not be able to certify for the CE mark after 31 December 2020.

The current plan is for the UKCA framework to align with the existing medical device regulations - the process which currently governs the CE-Marking Process. This means the rules for putting a product on the market in the UK may remain very similar to the approach currently in place in the short term.

UK notified bodies will be allowed to grant UKCA approvals from January 2021 as well as provide conformity assessment services for the NI market. From July 2023, the UK will stop recognising CE Markings, meaning that any medical device used in the UK will need to go through the UKCA marking process by then if it is to be used beyond July 2023, whether or not it is already in use.

It is the MHRA's stated ambition to establish a new approval pathway for software/AI in collaboration with key partners.

Meanwhile, the EU plans to upgrade CE marking requirements when the new Medical Devices Regulations (MDR) come into force in the EU from May 2021. These are generally considered more stringent than the MDD.

10. Interoperability and open standards

Ensure that the product makes the best possible use of open standards to ensure data quality and interoperability

Where healthcare technologies cannot 'talk' to each other, the result is often that information gets stuck in silos that create barriers to appropriate data sharing. This has a direct negative impact on patient care and the ability of clinicians to do their job safely and effectively.

To provide a seamless care journey, it is important that relevant technologies in the health and social care system are interoperable, in terms of hardware, software and the data contained within. For example, it is important that data from a patient's ambulatory blood glucose monitor can be downloaded onto appropriate clinical systems without being restricted to one type. Those technologies that need to

interface with clinical record systems must also be interoperable (https://service-manual.nhs.uk/service-standard/17-make-your-service-interoperable). NHS Digital hosts an Interoperability Toolkit (https://digital.nhs.uk/services/interoperability-toolkit) to support innovators.

Read more on interoperability:

- NHS England interoperability standards (https://www.england.nhs.uk/digitaltechnology/info-revolution/health-and-care-data/interoperability/)
- UK government open standards (https://www.gov.uk/government/publications/open-standards-for-government)

It is also important that data is recorded in a particular standardised way as this allows useful information to be gathered from multiple sources, to join up care. This can be achieved by following open standards. Within the English health and social care system, information standards (https://digital.nhs.uk/data-and-information/information-standards) cover the specifications used to collect and extract data from information technology systems.

It is necessary to demonstrate that a health technology - and its back-end systems - share data with other clinical systems within the appropriate rules regarding the capture, presentation, sharing and storage of data.

If a technology needs to communicate with clinical systems to share data, it must comply with the relevant clinical, professional and technical standards. There are standards that create a common ‘language’ in the recording of healthcare data and digital health technologies must use these.

Data standards

Digital and data-driven technologies should use the following standards or datasets in choosing data items or definitions:

- For patient/clinical/professional records, see the PRSB standards (https://theprsb.org/standards/):
  - Ambulance handover standard (https://theprsb.org/standards/ambulancehandover/)
  - Clinical referral standard (https://theprsb.org/standards/clinicalreferral/)
  - Core information standard (https://theprsb.org/standards/coreinformationstandard/)
  - Crisis care (https://theprsb.org/standards/crisiscare/)
  - Digital care and support plan (https://theprsb.org/standards/dcsp/)
  - Document naming standard (https://theprsb.org/standards/documentnaming/)
  - Healthy child record (https://theprsb.org/standards/healthychildrecordstandard/)
  - E-discharge (https://theprsb.org/standards/edischargesummary/)
  - Emergency care discharge (https://theprsb.org/standards/emergencycaredischarge/)
  - Maternity record standard (https://theprsb.org/standards/maternityrecordstandard/)
  - Mental health inpatient discharge (https://theprsb.org/standards/mentalhealthdischarge/)
  - Pharmacy information flows (https://theprsb.org/standards/pharmacyinformationflows1and2/)
  - Outpatient letters (https://theprsb.org/standards/outpatientletterstandard/)
  - Social care assessment standard (ADW) (https://theprsb.org/standards/adw/)
  - PRSB standards for the structure and content of health and care records (https://theprsb.org/standards/healthandcarerecords/)

- For coding of clinical data: SNOMED CT and SNOMED refsets (https://termbrowser.nhs.uk/?)
- For coding of clinical conditions and procedures: ICD-10 and OPCS4
- GS1 (https://www.gs1uk.org/our-industries/healthcare/gs1-standards-for-nhs-acute-trusts) – this is part of Scan4Safety
- Dm+d (the dictionary of medicines and devices) (https://www.nhsbsa.nhs.uk/pharmacies-gp-practices-and-appliance-contractors/dictionary-medicines-and-devices-dmd). The dm+d is a dictionary of descriptions and codes which represent medicines and devices in use across the NHS. Currently, only medicines are represented
- Other datasets which are not national standards but used in national applications in relevant fields. See Open standards for government (https://www.gov.uk/government/publications/open-standards-for-government)
- HTML5 for web sites
- Schema.org metadata
- Unicode for text
- WCAG 2.1 for accessibility
- ISO-8601 for timestamps in data
- OpenAPI v3 for documentation of REST APIs
- OAuth, OpenID Connect, FIDO for authentication
- HL7 v 2 and v 3
- FHIR+ FHIR Care Connect
- DICOM (https://www.dicomstandard.org/current/)
- Standards that have been mandated for use in the NHS in England through an Information standards notice (ISN (https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/information-standards-notices))
- NHS Data Dictionary (https://www.datadictionary.nhs.uk/). The NHS Data Model and Dictionary provides a reference point for approved Information Standards Notices to support health care activities within the NHS in England. It has been developed for everyone who is actively involved in the collection of data and the management of information in the NHS.

For more information, see open standards for government data (https://www.gov.uk/government/collections/open-standards-for-government-data-and-technology) and technology.

For implementation guidance, digital and data-driven technologies must follow the standards set out on the NHS Developer site. (https://developer.nhs.uk/)

If the technology is a wearable, a device, or integrates with either, then evidence must be provided of compliance with ISO/IEEE 11073 (https://ec.europa.eu/eip/ageing/standards/healthcare/e-health/isoiee-11073_en) Personal Health Data (PHD) Standards.

APIs

For APIs, follow the Government Digital Service's Open API Best Practices (https://www.gov.uk/guidance/gds-api-technical-and-data-standards).

There should be minimal barriers to entry to individuals who wish to read their own data.

Third parties must be given reasonable access to APIs in order to integrate their technology with yours.

The API must be documented and that documentation must be freely available.

Open source

Use standard open source libraries for generating and parsing data in an open format.

Ensure that the source code is open in order to facilitate auditing of how data is parsed.

11. Generate evidence that the product achieves clinical, social, economic or behavioural benefits

When building or developing the technology, consider what function the product delivers – this will inform the evidence generation plan. It's advisable to consider the generation of evidence as something that happens in parallel with the development of the product and builds throughout the product's life.

The first step in evidence generation may be proving that the product performs appropriately for its intended use at the bench - this is verification testing (see principle 4).

The product must then be validated which usually involves being tested in a setting that represents the intended population and/or environment. If preparing a submission for CE marking, this evidence would form the basis of the Clinical Evaluation Report. Remember to seek appropriate ethics approvals prior to accessing patient data for any evidence-generating studies. Public Health England has created a step-by-step guide to evidence generation for digital products (https://www.gov.uk/government/collections/evaluating-digital-health-products).

If evidence generation is at an early stage, the Academic Health Science Networks can provide support and guidance. The National Institute for Health and Care Excellence (NICE) has created the META (https://meta.nice.org.uk/) tool to help companies understand the kind of evidence needed to create a convincing case to commissioners,

Products aiming for national recommendation or procurement may be reviewed by NICE. NICE reviews require innovators to supply a greater body of evidence. They look at clinical effectiveness as well as economic impact.

A recommendation in NICE guidance represents the gold standard. Technologies must meet core eligibility criteria and demonstrate substantial benefit to patients or the health and care system. They must also be able to evidence those benefits. Issuing guidance will only be considered where it would mean faster and more consistent adoption of the technology.

NICE has developed an Evidence Standards Framework for digital health technologies (https://www.nice.org.uk/about/what-we-do/our-programmes/evidence-standards-framework-for-digital-health-technologies), working in close collaboration with NHS England, NHS Digital, Public Health England, MedCity and other stakeholders.

The framework has 3 components:

- evidence for effectiveness, based on the functional classification of the digital health technology for its intended use(s)
- evidence for economic impact

- supporting resources, including case studies

These standards inform technology developers and evaluators about which types of evidence should be generated, taking into account the functions and intended use of the product and its overall economic impact. A downloadable template is available to help with budget impact analysis.

NICE has devised a functional categorisation of digital tools into ‘tiers’ whereby the functions can be graded in terms of clinical impact and risk of harm. The level of evidence expected increases as the risk associated with the technology grows. For those products that perform more than one function, the evidence requirements for the function that carries the highest potential impact and highest potential harm should be met.

NICE’s technology evaluation programmes, such as Medical Technologies Evaluation Programme (https://www.nice.org.uk/About/What-we-do/Our-Programmes/NICE-guidance/NICE-medical-technologies-evaluation-programme) (MTEP), consider products that could offer substantial benefits to patients and the health and social care system over current practice.

Evidence based on independent research will score highly on assessment.

12. Define the commercial strategy

Innovators must take into account additional considerations when NHS data forms the basis of the commercial arrangements. These partnerships can be complex, so should not be undertaken lightly. The Department of Health and Social Care (DHSC) has set out 5 guiding principles (https://www.gov.uk/government/publications/creating-the-right-framework-to-realise-the-benefits-of-health-data) to ensure that the NHS, patients and the public gain fair benefit from agreements involving the sharing of health and care data. Innovators must use these five principles to inform their commercial approach with the NHS.

Ultimately, any commercial arrangement should fairly allocate the benefits between parties based on their respective contributions, roles, responsibilities, risks and investment. If an NHS data asset is being used to the benefit of a technology developer, the NHS and tech development must each undertake a comprehensive consideration of what constitutes ‘fair value’. Value should be considered in a holistic way, taking into account the potential financial value that may arise, as well as in-kind benefits to the NHS such as early access to new technologies or insight that might help the NHS run more effectively or efficiently. It can also be important to consider when negotiating commercial arrangements the APIs, open standards and levels of access needed to the output fit into the ecosystem (see section 10).

There are further considerations when a technology includes AI. We need to be assured that any products NHS organisations use meet the highest standards of safety and effectiveness. NHSX’s Buyer’s Guide to AI in Health and Care (https://www.nhsx.nhs.uk/ai-lab/explore-all-resources/adopt-ai/a-buyers-guide-to-ai-in-health-and-care/) contains a framework of questions that NHS organisations will be considering when entering into this type of transaction.

NHSX has set up the Centre for Improving Data Collaboration to facilitate data partnerships between the NHS and industry. The centre will provide specialist commercial and legal advice to NHS organisations entering commercial agreements; develop tools and exemplar contractual wording; and ensure that the advantages of scale in a single-payer health system deliver benefits for UK patients. The centre can be contacted at improvingdatacollaboration@nhsx.nhs.uk.

Innovators may also find the following papers useful when considering fair value and commercial models in relation to NHS data:

- Imperial: NHS data: maximising its impact on the health and wealth of the United Kingdom (https://spiral.imperial.ac.uk/handle/10044/1/76409)
- Reform: Making NHS data work for everyone (https://reform.uk/research/making-nhs-data-work-everyone)
- Future Care Capital: Taking next steps to harness the value of health and care data (https://futurecarecapital.org.uk/research/22nd-may-2019-taking-next-steps-to-harness-the-value-of-health-and-care-data/)
- Understanding Patient Data: research and resources (https://understandingpatientdata.org.uk/research-resources)

Print this page