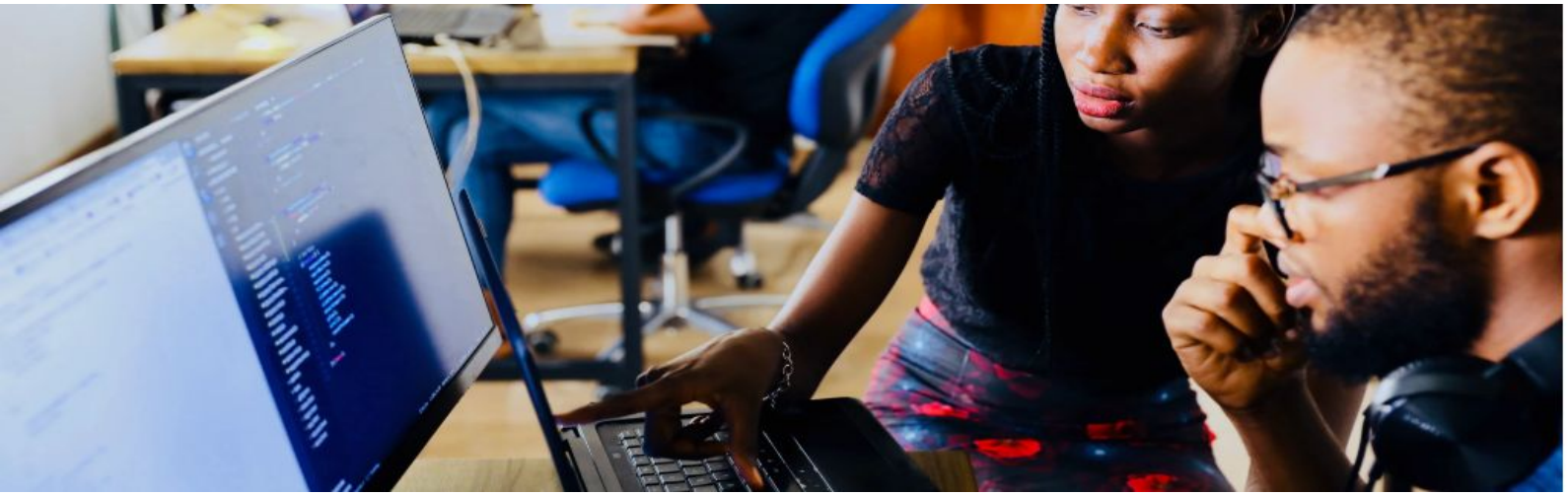
NHS Digital Health Technology Standard

Draft



NHS Digital Health Technology Standard

Draft

Publishing approval number: 001524

Version number: 1

First published: 24 February 2020

Prepared by: Rhod Joyce, Head of Partnerships, NHSX

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact communications@nhsx.nhs.uk

Contents

Background

NHSX is determined to improve health and social care by giving people the technology that they need. The NHS Long Term Plan sets out that future models will be underpinned by digitally-enabled care, and the Secretary of State's Technology vision sets the foundation for a new generation of digital services focused on user need, privacy and security, interoperability and inclusion.

This requires ensuring that digital health technologies that improve care, health outcomes or aid the system, are able to reach service users, patients, carers, clinicians and the wider workforce as easily as possible without safety being compromised.

The issue

There is frustration with the current way the NHS assesses digital health apps and tools. It's complicated and the NHS is not able to review the hundreds of technologies quickly enough, so that patients and staff can use them safely and appropriately.

The solution

NHSX has developed an open Digital Health Technologies Standard, based on existing industry and health standards, encompassing efficacy, safety, security, data protection, robustness, stability, interoperability, usability, accessibility and responsibility. It combines elements of the existing Digital Assessment Questions with other data and interoperability standards. We will also put in place a clear process for reviewing, assessing and evaluating digital health technologies that claim to meet this standard.

This is intended to speed up and streamline how health technologies are reviewed and commissioned by the NHS and social care, and enable innovation to flourish.

Survey

We recognise the need to co-develop these with stakeholders including developers, clinicians, commissioners and patient groups, before the planned introduction of the standard later in 2020.

We would like your feedback on the standard via our short survey to ensure it is robust, proportionate and attainable. The consultation runs until Wednesday 22 April 2020.

1. Review the Code of Conduct for Data-Driven Health and Care Technologies and, as appropriate, abide by the principles

Rationale

While data-driven health and care technologies will have the potential to deliver significant benefits to patients, clinicians, carers, service users and the system as a whole, it is our duty as the NHS and central government to capitalise on these opportunities responsibly. If we do not think about issues such as transparency, accountability, safety, efficacy, explicability, fairness and bias, it is also possible that the increasing use of data-driven technologies, including AI, within the health and care system could cause unintended harm.

The code of conduct clearly sets out the behaviours we expect from those developing, deploying and using data-driven technologies,and to ensure that everyone abides by the ethical principles for data initiatives developed by the Nuffield Council on Bioethics. These are:

- Respect for persons
- Respect for human rights
- Participation
- Accounting for decisions

Guidance

Read the Code of Conduct for Data-Driven Health and Care Technologies.

If conducting research with medical data, seek approval from the Health Research Authority (HRA) to carry out this research. This can be facilitated through the Integrated Research Application System (IRAS). For further information see the HRA information on data-driven technology.

If the patient data planning to be used has been anonymised in line with the ICO's code of conduct on anonymisation and meets the requirements of the common law duty of confidentiality, ethical review from the HRA will not be needed. However, HRA approval may still be required.

Conform to the UK Policy Framework for Health and Social Care Research.

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

Rationale

It is imperative that DHTs have a clear purpose. Developers must understand how their innovation or technology will result in better provision and/or outcomes for people and the

health and care system. DHTs must have a clear value proposition with a business case highlighting outputs, outcomes, benefits and performance indicators.

Developers must work with users to set out clear and defined user needs. Users may be patients, family, carers or staff. Their needs may be:

- Clinical
- Practical
- Emotional

Developers must regularly work with users to assess the design and performance of their DHTs, and have a mechanism for ensuring that those assessments inform future iterations.

Developers must set out a hypothesis for how the DHT will contribute to the provision of better care and/or improved health outcomes, for example through:

- Improvements in patient experience and outcomes
- Generation of new knowledge and capabilities
- Generation of a firmer evidence base, and reduction in uncertainty
- Efficiency improvements

Developers must clearly define measures that will be used to assess the outputs, outcomes and benefits of the DHT. They must publish performance against these KPIs openly and regularly alongside the assessment methodology, which should be linked back to the user need that is being addressed.

In addition to demonstrating user or system benefit, developers must outline where and how cost savings or reductions are likely to be made as a result of the use of their DHT in a health and care setting.

For this purpose, developers must also demonstrate that:

- Relevant clinical expertise has been involved in the design, testing and sign off of the product
- DHT Functionality is fit for purpose and is based upon NICE best practice guidance
- Source data is medically valid and up to date and has a plan to ensure that it remains up to date
- Outcomes have been exhaustively tested and proven (as far as is possible and proportionate)
- Post market surveillance is undertaken and feedback is risk assessed and acted upon.

Guidance

Read point 1 of the GDS Service Standard
Read point 10 of the GDS Service Standard.

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

Rationale
Health and care services are for everyone, including people with different physical, mental health, social, cultural or learning needs. All DHTs should be designed to meet the needs of this diverse set of users.

DHTs must be centred around specifically defined user needs and be:

- Easy to understand
- Easy to operate
- Informative

Guidance

DHTs must meet the following standards.

- Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems ISO 9241-210:2010
- Applying human factors ot medical devices
- Web Content Accessibility Guidelines (WCAG) and have evaluated their product with users during all stages of development and deployment.

Developers must also evidence facilitation of user feedback and a process of evaluation and release of appropriate updates.

Read information on the progressive web app checklist.
Read information on how to write an accessibility statement.

4. Ensure that the product is clinically safe to use

Rationale
All DHTs must be clinically safe to use and be designed in a way that ensures there is no risk of them causing harm to users, for instance by miscalculating a drug dose or giving incorrect medical advice to a citizen or health care professional. Safety must also not be compromised by the instability of the DHT.

Guidance

Developers must demonstrate that, for each of their DHTs:

- Authorship of data sources is up to date and recognised as expert clinical best practice
- Functionality is developed from best practice guidance and is fit for purpose
- Outcomes have been exhaustively tested and proven (as far as is possible and proportionate)

Developers must outline how their DHTs:

- Have plans and policies to limit and mitigate risk
- Any risks that the app could pose to people's health if it crashes or is used incorrectly

It must be shown that the following criteria are met.

- Clinical Risk Management Standard DCB0129.
- Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems DCB0160
- NHS England mandated Safety Standards (SCCI0129)
- ISO 14971 Medical Devices - Application of risk management to medical devices
- Relevant Health and safety standards for the setting

Evidence must be shown of:

- Origin and provenance of data sources
- Details of clinicians involved and their relevant professional registration

Read information on PD IEC/TR 80002-1 Medical device software Part 1: Guidance on the application of ISO 14971 to medical device software

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

Rationale

Innovators in the digital health field come from sectors that are not necessarily familiar with medical ethics and research regulation, and who may utilise data sets and processing methods that sit outside existing NHS safeguards.

It is our duty to ensure that the opportunities created by innovators are used responsibly. People need to know that their data is being used to improve health and care for them or others and that their privacy and rights are safeguarded. They need to understand how and when data about them is shared, so that they can feel reassured that their data is being used for public good, fairly and equitably.

Guidance

Everyone responsible for using personal data (as defined on the ICO's website) has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Developers must ensure that their DHTs meet the principles and requirements of The Data Protection Act, which treats health data as special category data. DHTs must use data in a way that is proportional. In particular, careful consideration should be given to the linkage of data, which may result in date becoming identifiable. Developers must be able to guarantee

that data linkage does not provide access to patient data to those who did not have the legal right.

It is important that the end user understands what the DHT will do with any data they provide, why it has been collected and how its use is meeting the defined user need(s) and purpose of the product. The user must be able to give 'informed consent' to the use of their personal identifiable data. If consent is not sought, there must be another legal basis for collecting and processing the data, such as approval under section 251 of the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002.

The DHT terms and conditions must set out clearly and simply exactly what will happen to user data, who it will be shared, and in what form it will be stored. As a minimum, it must comply with NHS Information Governance requirements.

The way that developers and their DHTs use NHS data, must be compliant with the national data opt-out policy.

If data persistence is unavoidable, or multiple copies of the original data are made, the drivers, requirements and benefits of these additional copies or persistent data must be set out and justified.

Developers must ensure that they are aware of the limitations of the data and assess: quality, completeness, presence of bias and the impact of their coding choices (e.g. efficiency vs. reproducibility).

In the case of machine learning, developers must 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. They must demonstrate whether the algorithm is published in a real-world deployed environment or a training environment.

As DHTs often rely on continuous deployment, and continuous software updates, and because there are risks of algorithmic drift, DHTs must have continuous anomaly detection in place to provide alerts to changes in a data source.

Developers must provide a:

- Data flow map
- Data protection impact assessment (DPIA)
- Data sharing agreement
- Privacy notice

Further information

- The Information Commissioner's Office (ICO) Guide to data protection
- Records Management Code of Practice for Health and Social Care 2016
- The Information Security Management: NHS Code of Practice
- NHS cloud services and data sharing guidance
- European Union Privacy Code of Conduct on Mobile health Apps
- The British Standards Institute PAS 277:2015 "Health and Wellness Apps - Quality criteria across the lifecycle - code of practice

- International Standard IEC 82304-1
- NHS England and NHS Innovation and the UK Statistics Authority guidance on data quality
- Department of Culture, Media and Sport Data Ethics Framework

6. Ensure that the product meets industry best practice security standards

Rationale

A core element of at-scale adoption and uptake is ensuring trust through security and data protection. Security decisions must not be an afterthought, but made throughout the development process in a rational way based on real-world testing. All DHTs must ensure that user data is collected, transmitted and stored safely.

Guidance

Developers must complete the NHS Digital Data Security and Protection Toolkit to provide assurance that they are practising good data security and that personal information is handled appropriately.

DHTs must be built to the required standards and tested for completeness and consistency with the OWASP Application Security Verification Standard (ASVS)

The mobile security standards include a number of checks to show that DHT processes and architecture are secure. This applies to the collection, transmission and storage of user data (both data *about* the user and data *generated* by the user).

DHTs will need to demonstrate that all security concerns and vulnerabilities are addressed, and explain how this has been done.

The Data Controller must ensure that data are processed (stored) in the UK, EU or a country deemed 'adequate' i.e. recognised by the EU Commission to have an adequate level of protection or in the USA under a Privacy Shield arrangement. They must have clear oversight of the actions of the Data Processor and remain accountable. Further information is available in NHS cloud services and data sharing guidance.

DHTs must ensure 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.

Further information

- OWASP Mobile Security Testing Guide (MSTG).
- OWASP Application Security Verification Standard (ASVS)
- Information on CREST accredited companies
- NHS Digital's Data Security Knowledge Library
- Department for Digital, Culture, Media and Sport code of practice for consumer 'internet of things' (IoT) security

7. Ensure that the product meets all regulatory requirements

Rationale

The regulation of health apps provides patients and healthcare professionals with the assurance that apps are high quality, safe and ethical.

Guidance

DHTs may need to conform to regulation. The two main types of regulation are:

1. Medical device regulation

If the DHT meets the definition of a medical device, then it must be registered with the Medicines and Healthcare Products Regulatory Agency (MHRA) and have a CE mark. Software that meets the definition of a medical device will be regulated as such. The new EU regulations on medical devices and in vitro medical devices will apply from May 2020.

2. Health and care service regulation: Care Quality Commission (CQC) registration

If the DHT provides a health or social care service that fits in one of the 14 regulated activities, there is a requirement to register with the CQC.

If the DHT constitutes a pharmacy service it requires General Pharmaceutical Council registration.

If the DHT forms part of a service that requires registered healthcare professionals to operate, registered healthcare professional status and names must be provided.

Further Information

- Guidance for registered pharmacies providing pharmacy services at a distance, including on the internet
- Information on Electronic Prescription Services
- The British Standards Institute PAS 277:2015 Health and Wellness Apps - Quality criteria across the lifecycle - code of practice
- BS EN 62304:2006 Medical Device Software - Software life-cycle processes
- ISO 13485 Medical Devices - Quality Management Systems - Requirements for regulatory purposes

8. Ensure that the product makes the best possible use of open standards and comply by all relevant technical standards

Rationale

If a DHT needs to communicate with clinical systems to share data, it must comply with the relevant clinical, professional and technical standards. For example, this will be necessary if

a DHT writes clinical information in records held by GPs, or allows users to access their own records.

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

Guidance

DHTs should use the following standards or datasets in choosing data items or definitions:

Data standards

- Standards that have been mandated for use in the NHS in England through an Information standards notice (ISN)
- PRSB standards for content of patient/clinical/professional records
- NHS Data Dictionary
- SNOMED CT and SNOMED refsets.
- ICD-10 and OPCS4 (coding systems for diseases and procedures)
- GS1 for barcoding
- Dm+d (the dictionary of medicines and devices)
- Other datasets which are not national standards but used in national applications in relevant fields
- Global data standards
    - 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 FHIR+ FHIR Care Connect

For technical standards, DHTs must follow the standards set out on the NHS Developer site.

APIs must meet the Government Digital Services: Open API Best Practices.

If the DHT is a wearable or device or integrates with them, they must provide evidence of compliance with ISO/IEEE 11073 Personal Health Data (PHD) Standards.

All apps must meet criteria covering:

- Data sharing
- Service level agreements for your services and APIs
- Reliance on third-party services

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

Rationale

All DHTs must be suitable for their stated purpose and be confident that they can provide a robust and stable service. They must have been effectively tested for reliability, performance and scalability.

There should also be a plan that explains how the DHT will continue to be developed and managed, including 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.

It must also be proven that the DHT has the ability to rollback to a previous version, should any significant problems be encountered following an update, and how any risk to patient data and, more importantly, patient health, will be limited and mitigated and a recovery plan in the event of a catastrophic failure.

Guidance

DHT suppliers should have accreditation to an industry wide testing standard such as ISO 9001 or ISO 29119: Information on ISO standards.

All apps must show that they meet criteria covering:

- Quality assurance
- Service management
- Product development

A DHT must demonstrate:

- Reliability: that it is capable of sustaining continued stress and load
- Performance: that it maintains responsiveness under various loading conditions
- Scalability: its ability to meet increased demand

This must cover both the DHT itself and any supporting infrastructure which it may rely on ie. web services.

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

Rationale

All DHTs must work and must be clear about their purpose and their benefits to citizens and health and social care professionals. They must be grounded in the best and most up-to-date knowledge, derived from research, clinical experience and citizen preferences; they must also ensure that they monitor their own efficacy so that they can evidence their impact.

Guidance

NICE has developed an Evidence Standards Framework which DHTs must comply with. The DHT is classified according to the NICE Evidence Tiers - evidence requirements are cumulative. The framework has three components:

- Evidence for effectiveness standards, based on the functional classification of the digital health technology for its intended use(s).
- Evidence for economic impact standards.
- Supporting resources, including case studies.

NICE's technology evaluation programmes, such as Medical Technologies Evaluation Programme (MTEP), consider products that could offer substantial benefits to patients and the health and social care system over current practice. 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, be able to evidence those benefits, guidance will only be considered where it would mean faster and more consistent adoption of the technology.

Many DHTs will be the subjects of commercial arrangements (see Making NHS data work for everyone, Figure 10 for examples) between NHS organisations and commercial organisations, the foundation of any commercial structure should be to ensure that the terms of the engagement fairly allocate the benefits between the parties based on their respective contributions, roles, responsibilities, risks and costs. When the basis or key component of the commercial arrangement is NHS data, it must adhere to the principles described in Creating the right framework to realise the benefits of health data.

Before entering into any commercial arrangement, the problems that need solving, and who for, including any long-term vision, should be fully understood by all parties. The relationship between the parties will be set out in a binding legal contract that will impact all parties both during and long after the lifetime of the contract. This will require legal advice.

Before engaging with the legal teams, the following should be considered:

- Proportionality
- Scope
- Exclusivity
- Value
- Ownership of intellectual property
- Liability
- Audit

- Bias
- Roles

Further Information

Read the NICE commissioned Evidence Generation Guide; Evidence Guide for App Developers; and Digital Health Evidence Case Studies produced by the York Health Economics Consortium.

Read the Oxford Centre for Evidence-based Medicine – Levels of Evidence (March 2009) Information on levels of medical evidence.

Evidence based on independent research will score highly on assessment.

Survey

The draft standard has been created in collaboration with stakeholders from across the digital health ecosystem. We now want to gather feedback from a wider range of voices who have an interest in digital health, including developers, clinicians, commissioners and patient groups, to ensure it is robust, ambitious and attainable.

We are seeking views on the proposed standard until Wednesday 22 April 2020, 11.59pm. The feedback we receive will directly contribute to the development of the standard. It will be published in Summer 2020, after which we will review and update it annually.

Have your say here