

THE NHS DTAC

**A SHORT GUIDE FOR
HEALTHTECH FOUNDERS.**



The following carousel has been adapted from this article:



The screenshot shows the top navigation bar of the Naq Cyber website. The logo 'naq.' is on the left, followed by menu items: 'Product', 'Solution', 'Resources', and 'Company'. A 'Book a demo' button is on the right. Below the navigation, the breadcrumb 'Blog > Healthcare' is visible. The main heading is 'A Guide to the NHS Digital Technology Assessment Criteria (DTAC)'. Below the heading is a short paragraph: 'As digital health solutions become integral to healthcare, compliance with DTAC's safety, security, usability, and accessibility standards is essential. Discover the ins and outs of the NHS Digital Technology Assessment Criteria in our comprehensive guide.'

Available here:

<https://www.naqcyber.com/blog/a-guide-to-the-nhs-digital-technology-assessment-criteria>

INTRODUCTION

Formally introduced in 2021, the NHS Transformation Directorate introduced the DTAC (Digital Technology Assessment Criteria) which aims to serve as the national baseline criteria for new and existing **digital health technologies** used within the NHS.

It brings together legislation and best practices in **five core areas**:

Clinical Safety

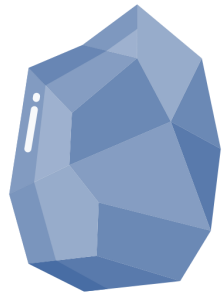
Data Protection

Technical Security

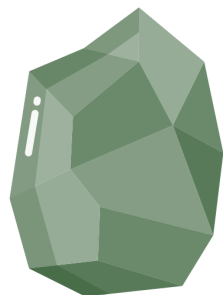
Interoperability

Usability and Accessibility

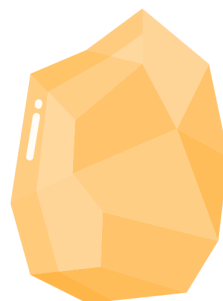
The scope of the framework is expansive and requires meeting compliance with **additional standards** such as the:



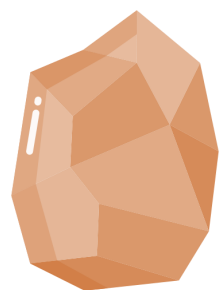
DCB0129/0160



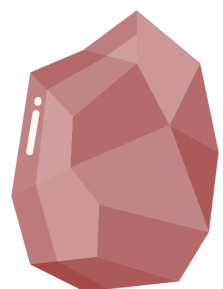
NHS DSPT



UK GDPR



Cyber Essentials



MHRA regulation

IMPORTANT NOTE.

Unlike frameworks like the NHS Data Security and Protection Toolkit, no formalised **DTAC assessment or certification process** is currently available.

Instead, developers must complete the DTAC questionnaire and **submit all relevant evidence directly to the buyer** for assessment.

Because there is no centralised DTAC function for all applications, developers must first **clarify who will conduct the review.**

This may be the specific buyer, such as an **individual trust or an integrated care system.**



1.

**CLINICAL
SAFETY**

CLINICAL SAFETY

Paramount to the safe deployment of digital health technologies in the healthcare setting is **CLINICAL SAFETY**. This core aspect rightfully takes the first consideration in the NHS DTAC.

The NHS has two standards for clinical safety: **DCB0129** and **DCB0160**.

These two standards have **almost identical requirements**. However:

DCB0129 applies to the developer of the health solution,

DCB0160 applies to the organisation buying or implementing the healthcare technology, such as the NHS trust.

DCB 0129

To comply with the standard, manufacturers needs to undertake a formal risk assessment on the product and produce **three documents** summarising the outcome:



Clinical Risk Management Plan



Hazard Log



Clinical Safety Case Report.

Note that DCB 0129 is **supplemental** to the requirements of the NHS Information Governance Toolkit and the Medical Device Directive/Regulation.

DTAC Questions for Clinical Safety

Have you undertaken Clinical Risk Management activities for this product which comply with **DCB0129**?

Please detail your **clinical risk management system**

Please supply your **Clinical Safety Case Report** and **Hazard Log**

Please provide the name of your **Clinical Safety Officer (CSO)**, their profession and registration details

If your product falls within the UK Medical Devices Regulations 2002, is it registered with the **Medicines and Healthcare products Regulatory Agency (MHRA)**?

If yes, please provide your **MHRA registration number**

If the UK Medical Device Regulations 2002 are applicable, please provide your Declaration of Conformity and, if applicable, **certificate of conformity issued by a Notified Body / UK Approved Body**

Do you use or connect to any **third-party products**?

If yes, please attach relevant **Clinical Risk Management documentation** and conformity certificate



2.

**DATA
PROTECTION**

DATA PROTECTION.

Patient data protection is tantamount as confidentiality is key for the patient provider relationship.

To meet the DTAC framework, suppliers and developers must adhere to NHS data protection standards, such as:

- . **The Caldicott Principles**
- . **10 Data Security Standards,**
- . **The UK-GDPR.**

Additionally, developers must conduct a **Data Protection Impact Assessment (DPIA)** to identify potential risks to individuals' rights and freedoms when using digital health technology.

DATA PROTECTION.

Solutions that process health information must register with the **ICO** (Information Commissioner's Office) and appoint a **Data Protection Officer**, which must be named within the DTAC documentation.

To meet the DTAC standard, developers must also comply with the **Data Security and Protection Toolkit**, an NHS framework applicable to all suppliers regardless of whether they provide digital health solutions.

The logo for the Information Commissioner's Office (ICO) features the lowercase letters 'ico.' in a bold, dark blue, sans-serif font. The 'i' has a dot above it, and the 'o' has a dot to its right.

Information Commissioner's Office

The NHS logo consists of the letters 'NHS' in a bold, white, sans-serif font, set against a blue rectangular background.

England

Data Security and Protection Toolkit

DTAC Questions for Data Protection (Part 1)

If you are required to register with the **Information Commissioner**, please attach evidence of a current registration.

If you are not required to register, please attach a completed self-assessment showing the outcome from the Information Commissioner and your responses which support this determination.

Do you have a nominated **Data Protection Officer (DPO)**?

If you are required to have a nominated Data Protection Officer, please provide their name.

If you are not required to have a DPO please attach a **completed self-assessment** showing the outcome from the Information Commissioner and your responses which support this determination.

Does your product have **access to any personally identifiable data** or NHS held patient data?

DTAC Questions for Data Protection (Part 2)

Please confirm you are compliant (having standards met or exceeded status) with the annual **Data Security and Protection Toolkit Assessment**.

If you have not completed the current year's assessment and the deadline has not yet passed, please confirm that you intend to complete this ahead of the deadline and that there are no material changes from your previous years submission that would affect your compliance.

Please attach the **Data Protection Impact Assessment (DPIA)** relating to the product.

Please confirm your risk assessments and mitigations / access controls / system level security policies **have been signed-off by your Data Protection Officer** (if one is in place) or an accountable officer where exempt in question C2.2.

Please confirm **where you store and process data** (including any third-party products your product uses)

If you process **store or process data outside of the UK**, please name the country and set out how the arrangements are compliant with current legislation



3.

**TECHNICAL
SECURITY**

TECHNICAL SECURITY

To protect sensitive healthcare data, digital health technologies must be stable, secure, and continuously developing in line with best practices and new **cybersecurity requirements**.

To ensure this, the DTAC evaluates the **technical assurance of products**, assessing their security measures and ability to mitigate potential vulnerabilities.

The technical security section of the Digital Technology Assessment Criteria requires businesses to provide proof of **Cyber Essentials Certification**.



TECHNICAL SECURITY

The Cyber Essential scheme was developed by the UK government to ensure businesses have the necessary basic security measures to protect the UK supply chain from emerging cyber threats.

In addition to this, the DTAC also requires digital health solutions to have **strong security measures**, such as Multi-Factor Authentication, custom code security review, and proof of an annual penetration test.



DTAC Questions for Technical Security

Please attach your **Cyber Essentials Certificate**

Please provide the summary report of **an external penetration test of the product** that included Open Web Application Security Project (OWASP) Top 10 vulnerabilities from within the previous 12-month period.

Please confirm whether **all custom code had a security review.**

Please confirm whether all privileged accounts have appropriate **Multi-Factor Authentication (MFA)?**

Please confirm whether **logging and reporting requirements** have been clearly defined.

Please confirm whether the product **has been load tested.**



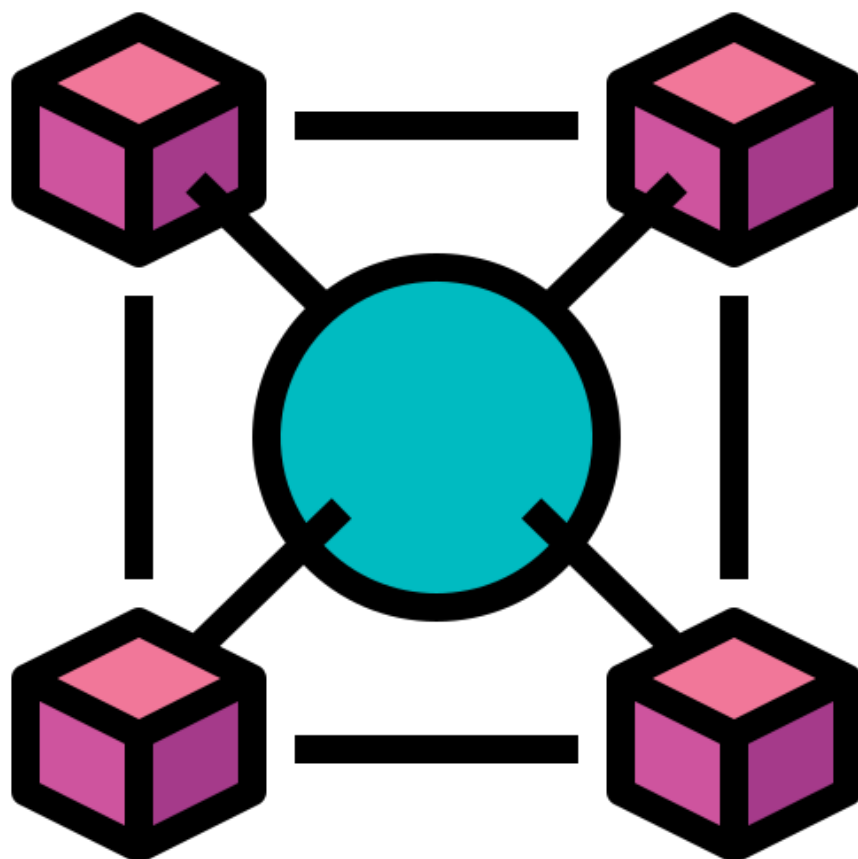
4.

**INTER-
OPERABILITY**

INTEROPERABILITY

Effective communication and data exchange between healthcare systems is crucial for seamless and coordinated care delivery.

The DTAC assesses the interoperability of products, ensuring that data can be communicated **accurately, quickly, and securely to NHS systems** while adhering to the security standards mentioned above.



DTAC Questions for Technical Security (Part 1)

Does your product expose any **Application Programme Interfaces (API)** or integration channels for other consumers?

If yes, please provide detail and evidence:

The API's (e.g., what they connect to) set out the healthcare standards of data interoperability e.g., **Health Level Seven International (HL7) / Fast Healthcare Interoperability Resources (FHIR)**

Confirm that they follow Government Digital Services Open API Best Practice

Confirm they are documented and freely available

Third parties have reasonable access to connect

If no, please set out why your product does not have APIs.

Do you use **NHS number** to identify patient record data?

If yes, please confirm **whether it uses NHS Login** to establish a user's verified NHS number.

If no, please set out the rationale, how your product established NHS number and the associated security measures in place.

DTAC Questions for Technical Security (Part 2)

Does your product have the capability for **read/write operations with electronic health records (EHRs)** using industry standards for secure interoperability (e.g. OAuth 2.0, TLS 1.2)

If yes, please detail the standard

If no, please state the **reasons and mitigations**, methodology and security measures.

Is your product a **wearable or device**, or does it integrate with them?

If yes, provide evidence of how it complies with **ISO/IEEE 11073 Personal Health Data (PHD)** Standards.



5.

USABILITY

&

ACCESSIBILITY

USABILITY AND ACCESSIBILITY

Digital health technologies should be **user-friendly** and accessible to all individuals.

The DTAC provides a **conformity rating** for usability and accessibility, benchmarking products against good practice and the **NHS Service Standard**.

This ensures that products are designed with users' needs in mind, **including those with disabilities**.



DTAC Questions for Usability and Accessibility (Part 1)

Understand users and their needs in context of health and social care

Do you engage users in the development of the product?

If yes or working towards it, how frequently do you consider user needs in your product development and what methods do you use to engage users and understand their needs?

Work towards solving a whole problem for users

Are all key user journeys mapped to ensure that the whole user problem is solved, or it is clear to users how it fits into their pathway or journey?

If yes or working towards it, please attach the user journeys and/or how the product fits into a user pathway or journey

Make the service simple to use

Do you undertake **user acceptance testing** to validate usability of the system?

If yes or working towards it, please attach information that demonstrates that user acceptance testing is in place to validate usability.

DTAC Questions for Usability and Accessibility (Part 2)

Make sure everyone can use the service

Are you international **Web Content Accessibility Guidelines (WCAG) 2.1** level AA compliant?

Provide a link to your published accessibility statement.

Create a team that includes multi-disciplinary skills and perspectives

Does your team contain **multidisciplinary skills**?

Use agile ways of working

Do you use agile ways of working to deliver your product?

Iterate and improve frequently

Do you continuously develop your product?

Define what success looks like and be open about how your service is performing

Do you have **a benefits case that includes your objectives** and the benefits you will be measuring and have metrics that you are tracking?

DTAC Questions for Usability and Accessibility (Part 3)

Choose the right tools and technology

Does this product meet with **NHS Cloud First Strategy**?

Does this product meet the NHS Internet First Policy?

Use and contribute to open standards, common components and patterns

Are common components and patterns in use?

If yes, which common components and patterns have been used?

Operate a reliable service

Do you provide a **Service Level Agreement** to all customers purchasing the product?

Do you report to customers on your performance with respect to support, system performance (response times) and availability (uptime) at a frequency required by your customers?

Please attach a copy of the information provided to customers

Please provide your average service availability for the past 12 months, as a percentage to two decimal places.

IMPORTANT POINT.

It is crucial to note that every time **a new feature** is added to the digital health solution, **a new DTAC** must be submitted to ensure continuous compliance with the standards. This also includes **updating any DCB0129 documentation** to ensure that new features have undergone a clinical risk assessment.

Once evidence is submitted, the responsibility of assessing and determining whether a digital health solution meets the DTAC standard **lies on the buyer.**

If the evidence provided is insufficient, unclear or outdated, developers may **have to provide further clarification or evidence** before their submission is approved.

**Hope you found
this helpful!**



**This is a series we are making to help
HealthTech Innovators access better
resources.**

Just our small way of helping!