**The NELFT Digital Technology Assessment Criteria**

**for Health and Social Care (DTAC)**

[1. What is a DTAC form: 2](#_Toc94608158)

[2. How to complete: 2](#_Toc94608159)

[A. Company information - Non-assessed section 3](#_Toc94608160)

[B. Value proposition - Non-assessed section 4](#_Toc94608161)

[C. Technical questions - Assessed sections 5](#_Toc94608162)

[C1 - Clinical safety 5](#_Toc94608163)

[C2 - Data protection 9](#_Toc94608164)

[C3 - Technical security 11](#_Toc94608165)

[C4 - Technical Operation 13](#_Toc94608166)

[C5 - Interoperability criteria 15](#_Toc94608167)

[Please upload relevant supporting documentation 16](#_Toc94608168)

# What is a DTAC form:

The Digital Technology Assessment Criteria for health and social care (DTAC) gives staff, patients and citizens confidence that the digital health tools they use meet our clinical safety, data protection, technical security, interoperability and usability and accessibility standards.

The DTAC brings together legislation and good practice in these areas. It is the new national baseline criteria for digital health technologies entering into the NHS and social care.

The DTAC is designed to be used by healthcare organizations to assess suppliers at the point of procurement or as part of a due diligence process, to make sure new digital technologies meet our minimum baseline standards. For developers, it sets out what is expected for entry into the NHS and social care.

# How to complete:

The DTAC form provides a consistent question set and enables you to present your evidence as free text in the Options or Supporting Answer columns

* You should make sure your product meets the assessment criteria, gathering the required evidence
* You may choose to use a third party to do this for you.
* You may be asked to provide this evidence during the procurement process.

Please complete all question, inserting NA (Not applicable) to any question(s) that is not applicable to your organization.

Once completed, please return to [SoftwareRequest@nelft.nhs.uk](mailto:SoftwareRequest@nelft.nhs.uk)

# A. Company information - Non-assessed section

Information about your organization and contact details.

|  |  |  |
| --- | --- | --- |
| **Code** | **Question** | **Option** |
| A1 | Provide the name of your company | Free text |
| A2 | Provide the name of your product | Free text |
| A3 | Provide the type of product | App | Wearable | Software as a Service (SaaS) | Other |
| A4 | Provide the name and job title of the individual who will be the key contact at your organization – TECHNICAL CONTACT? | Free text |
| A5 | Provide the key contact's email address | Free text |
| A6 | Provide the key contact's phone number | Free text |
| A7 | Provide the registered address of your company | Free text |
| A8 | In which country is your organization registered? | Free text |
| A9 | If you have a Companies House registration in the UK please provide your number | Free text |
| A10 | If applicable, when was your last assessment from the Care Quality Commission (CQC)? | Date | Not applicable |
| A11 | If applicable, upload your latest CQC report. | Upload |

# B. Value proposition - Non-assessed section

Please set out the context of the clinical, economic or behavioral benefits of your product to support the review of your technology. These criteria will not be scored but will provide the context of the product undergoing assessment.

Where possible, please provide details relating to the specific technology and not generally to your organization.

|  |  |  |  |
| --- | --- | --- | --- |
| **Code** | **Question** | **Option** | **Supporting Answer** |
| B1 | Who is this product intended to be used for? | Patients | Diagnostics | Clinical Support | Infrastructure | Workforce | Other |  |
| B2 | Provide a clear description of what the product is designed to do and of how it is expected to be used | Free text |  |
| B3 | Describe clearly the intended or proven benefits for users and confirm if / how the benefits have been validated | Free text |  |
| B4 | Please attach one or more user journeys which were used in the development of this product  Where possible please also provide your data flows | Attached | Not available |  |

## 

## 

# C. Technical questions - Assessed sections

## C1 - Clinical safety

Establishing that your product is clinically safe to use.

You must provide responses and documentation relating to the specific technology product that is subject to assessment.

The DCB0129 standard applies to organizations that are responsible for the development and maintenance of health IT systems. A health IT system is defined as “product used to provide electronic information for health and social care purposes”. DTAC is designed as the assessment criteria for digital health technologies and C1 Clinical Safety Criteria is intended to be applied to all assessments. If a developer considers that the C1 Clinical Safety is not applicable to the product being assessed, rationale must be submitted exceptionally detailing why DCB0129 does not apply.

The DCB0160 standard applies to the organization in which the health IT is deployed or used. It is a requirement of the standard (2.5.1) that in the procurement of health IT systems the organization must ensure that the manufacturer and health IT system complies with DCB0129. The organization must do so in accordance with the requirements and obligations set out in the DCB0160 standard. This includes personnel having the knowledge, experience and competences appropriate to undertaking the clinical risk management tasks assigned to them and organizations should ensure that this is the case when assessing this section of the DTAC.

If the Clinical Safety Officer or any other individual has concerns relating to safety of a medical device including software and apps, this should be reported to the Medicines and Healthcare products Regulatory Agency (MHRA) using the Yellow Card reporting system: [Report a problem with a medicine or medical device - GOV.UK (www.gov.uk)](https://www.gov.uk/report-problem-medicine-medical-device).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Code** | **Question** | **Options** | **Supporting information** | **Supporting Answer** |
| C1.1 | Have you undertaken Clinical Risk Management activities for this product which comply with DCB0129? | Yes | No | The [DCB0129](https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems) standard applies to organisations that are responsible for the development and maintenance of health IT systems. A health IT system is defined as ‘“product used to provide electronic information for health and social care purposes”. |  |
| C1.1.1 | Please detail your clinical risk management system | Attached | No evidence attached | DCB0129 sets out the activities that must and should be undertaken for health IT systems.  An example [clinical risk management system template](https://digital.nhs.uk/services/clinical-safety/documentation#clinical-risk-management) can be downloaded from the NHS Digital website. |  |
| C1.1.2 | Please supply your Clinical Safety Case Report and Hazard Log | Attached | No evidence available | Specifically your DTAC submission should include:   * A summary of the product and its intended use * A summary of clinical risk management activities * A summary of hazards identified which you have been unable to mitigate to as low as it is reasonably practicable * The clear identification of hazards which will require user or commissioner action to reach acceptable mitigation (for example, training and business process change)   It should not include the hazard log in the body of the document - this should be supplied separately.  Example [Clinical Safety Case Report and Hazard Log templates](https://digital.nhs.uk/services/clinical-safety/documentation#clinical-risk-management) can be downloaded from the NHS Digital website. |  |
| C1.2 | Please provide the name of your Clinical Safety Officer (CSO), their profession and registration details | Free Text | The CSO must:   * Be a suitably qualified and experienced clinician * Hold a current registration with an appropriate professional body relevant to their training and experience * Be knowledgeable in risk management and its application to clinical domains * Be suitably trained and qualified in risk management or have an understanding in principles of risk and safety as applied to Health IT * Have completed appropriate training   The work of the CSO can be undertaken by an outsourced third party. |  |
| C1.3 | If your product falls within the UK Medical Devices Regulations 2002, is it registered with the Medicines and Healthcare products Regulatory Agency (MHRA)? | Yes | No | Not applicable | If this question is not applicable, because your product does not fall within the UK Medical Devices Regulations 2002, continue to question C1.4.  If No, but the product falls within the UK Medical Devices Regulations 2002, continue to question C.1.3.2.  The MHRA provides guidance on medical devices to place them on the market in Great Britain and Northern Ireland, [regulatory requirements](https://www.gov.uk/guidance/regulating-medical-devices-in-the-uk) for all medical devices to be placed on the UK market, [conformity assessment](https://www.gov.uk/guidance/medical-devices-conformity-assessment-and-the-ukca-mark) and the UK Conformity Assessed (UKCA) mark, [classification of stand-alone medical device software](https://www.gov.uk/government/publications/medical-devices-software-applications-apps) (including apps) and [how to tell if your product falls within the UK Medical Devices Regulations 2002](https://www.gov.uk/guidance/borderline-products-how-to-tell-if-your-product-is-a-medical-device). |  |
| C1.3.1 | If yes, please provide your MHRA registration number | Free text |  |  |
| C1.3.2 | 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 | Attached | No evidence available | Medical device manufacturers must ensure that their device complies with the relevant Essential Requirements of the legislation and draw up a Declaration of Conformity to declare this.  Class I devices with a measuring function and devices in Class IIa, IIb and III must undergo conformity assessment from an EU Notified Body or UK Approved Body which has been designated for medical devices, and be issued a certificate of conformity (commonly referred to as a “CE certificate” or “UKCA certificate”). |  |
| C1.4 | Do you use or connect to any third-party products? | Yes I No | If no, continue to section C2.  [DCB0129](https://digital.nhs.uk/services/clinical-safety/documentation#clinical-risk-management) contains the requirements in relation to third party products. |  |
| C1.4.1 | If yes, please attach relevant Clinical Risk Management documentation and conformity certificate | Attached | No evidence available |  |  |

## 

## C2 - Data protection

Establishing that your product collects, stores and uses data (including personally identifiable data) compliantly.

This section applies to most digital health technology products however there may be some products that do not process any NHS held patient data or any identifiable data. If this is the case, the Data Protection Officer, or other suitably authorized individual should authorize this data protection section being omitted from the assessment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Code** | **Question** | **Options** | **Supporting information** | **Supporting Answer** |
| C2.1 | 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. | Attached | Not provided | There are some instances where organizations are not required to register with the Information Commissioner. This includes where no personal information is being processed.  The Information Commissioner has a [registration self-assessment tool](https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/) to support this decision making. |  |
| C2.2 | Do you have a nominated Data Protection Officer (DPO)? | Yes  No  We do not need one | Not all organizations are required to have a [Data Protection Officer](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/#ib1) (DPO). This is determined by the type of organization and core activities. The most common reason for organizations providing digital health technologies to have a DPO is due to the core activities involving processing health data (being a special category).  The Information Commissioner has a [self-assessment tool](https://digital.nhs.uk/services/clinical-safety/documentation#clinical-risk-management) to determine whether you must appoint a DPO. |  |
| C2.2.1 | 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. | Free text | Attachment |  |  |
| C2.3 | Does your product have access to any personally identifiable data or NHS held patient data? | Yes | No | The UK General Data Protection Regulation (GDPR) applies to the processing of [personal data](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/).  If no, continue to question C2.4 |  |
| C2.3.1 | 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. | Confirmed | Unable to confirm | The [Data Security and Protection Toolkit](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit) allows organizations to measure performance against the National Data Guardian’s 10 data security standards. |  |
| C2.3.2 | Please attach the Data Protection Impact Assessment (DPIA) relating to the product. | Attached | Not provided | [DPIA’s](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) are a key part of the accountability obligations under the UK GDPR, and when done properly help organizations assess and demonstrate how they comply with data protection obligations.  The Information Commissioner has provided guidance on [how to complete a DPIA](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how9) and a [sample DPIA template](https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx). |  |
| C2.4 | 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. | Confirm | Cannot confirm |  |  |
| C2.5 | Please confirm where you store and process data (including any third-party products your product uses) | UK only | In EU | Outside of EU | Individual organizations within the Health and Social Care system are accountable for the risk-based decisions that they must take. |  |
| C2.5.1 | 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 | Free text | From 1 January 2021, the UK GDPR applies in the UK in place of the “EU GDPR’. The UK GDPR will carry across much of the existing EU GDPR legislation. The Department for Digital, Culture, Media & Sport has published two [Keeling Schedules](https://www.gov.uk/government/publications/data-protection-law-eu-exit) which show the changes to the Data Protection Act 2019 and EU GDPR.  The Information Commissioner has published guidance on [international data transfers](https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/international-data-transfers/) after the UK exit from the EU Implementation Period. |  |

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## C3 - Technical security

Establishing that your product meets industry best practice security standards and that the product is stable.

Dependent on the digital health technology being procured, it is recommended that appropriate contractual arrangements are put in place for problem identification and resolution, incident management and response planning and disaster recovery.

Please provide details relating to the specific technology and not generally to your organization.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Code** | **Question** | **Options** | **Supporting information** | **Supporting Answer** |
| C3.1 | Please attach your Cyber Essentials Certificate | Attached | No evidence available | [Cyber Essentials](https://www.ncsc.gov.uk/cyberessentials/overview) helps organizations guard against the most common cyber threats.  The National Cyber Security Centre (NCSC) have published [cyber security guidance for small to medium enterprises](https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations) (SME’s). |  |
| C3.2 | Please attach your ISO27001 Certificate | Attached | No evidence available | A key benefit that ISO 27001 certification provides is evidence of your compliance with information security to international standards which helps organisations guard against the most common cyber threats. |  |
| C3.3 | 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. | Attached | No evidence available | The NCSC provides guidance on [penetration testing](https://www.ncsc.gov.uk/guidance/penetration-testing). The OWASP Foundation provides guidance on the [OWASP top 10 vulnerabilities](https://owasp.org/www-project-top-ten/). |  |
| C3.4 | Please confirm whether all custom code had a security review. | Yes - Internal code review | Yes - External code review |  No | No because there is no custom code | The NCSC provides guidance on [producing clean and maintainable code](https://www.ncsc.gov.uk/collection/developers-collection/principles/produce-clean-maintainable-code). |  |
| C3.5 | Please confirm whether all privileged accounts have appropriate Multi-Factor Authentication (MFA)? | Yes | No | The NCSC provides guidance on [Multi-Factor Authentication](https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services). |  |
| C3.6 | If the solution under consideration is a cloud hosted SaaS please confirm whether user accounts have appropriate Multi-Factor Authentication (MFA)? | Yes | No | The NCSC provides guidance on [Multi-Factor Authentication](https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services). |  |
| C3.7 | Please confirm whether logging and reporting requirements have been clearly defined. | Yes | No | The NCSC provides guidance on [logging and protective monitoring](https://www.ncsc.gov.uk/collection/mobile-device-guidance/logging-and-protective-monitoring).  To confirm yes to this question, logging (e.g. audit trails of all access) must be in place. It is acknowledged that not all developers will have advanced audit capabilities. |  |
| C3.8 | Please confirm data encryption standards used in transit and at rest. | Data in transit Minimum requirement TLS1.2  Data at rest requirement AES256Bit |  |  |
| C3.9 | What precautionary measures are in place to ensure server, storage and network devices are up to date and not at risk of any cyber threats\attacks\Malware or viruses | Anti Virus  Firewalls  IPS\IDS  WAF  Backup Solutions |  |  |

## 

# C4 - Technical Operation

Establishing that your product meets NELFT’s best practice for Hardware and Software and that the product is stable.

Dependent on the digital health technology being procured, it is recommended that appropriate contractual arrangements are put in place for problem identification and resolution, incident management and response planning and disaster recovery.

Please provide details relating to the specific technology and not generally to your organization.

|  |  |  |  |
| --- | --- | --- | --- |
| **Code** | **Question** | **Options** | **Supporting Answer** |
| C4.1 | Does NELFT need to provide any Hardware for your system? | Please include details of Desktops\Server (VM\Physical) that would be required? | Please attach technical documentation |
| C4.2 | Is the expectation that the Hardware\devices will sit on NELFT’s network |  |  |
| C4.3 | Is there a specific cabling requirement (CAT5/CAT6(a) |  |  |
| C4.4 | Is there a specific bandwidth required by the Devices\Hardware | Please state a typical size of data packets |  |
| C4.5 | Are they any Dependencies? such as Java, active X |  |  |
| C4.6 | Are there any server requirement from NELFT | Please state if any disk space is required |  |
| C4.7 | Deployment type - server, client, Cloud, Web | Please state how you propose for your system to be deployed to NELFT |  |
| C4.8 | How often is the system updated? How are updates cascaded through the system | Version releases | Please state if local admin rights are required for any updates |
| C4.9 | How will data be backed up and what contingencies are in place if your data repository fails |  |  |
| C4.10 | Do you have HSCN |  |  |
| C4.11 | Do you need access Via RDP over HSCN |  |  |
| C4.12 | Are there any known Fixes |  |  |
| C4.13 | If On-Prem - How do you support the system remotely for issues(s) |  |  |
| C4.14 | Once the system has been deployed to NELFT, please state after go-live support | What is your support model, please attach any document | Please provide Service Level Agreements documentations |
| C4.15 | Does the support include a break fix element should hardware fail | Please provide Support contact Details |  |
| C4.16 | Is there a support and maintenance contract which entitles NELFT to future upgrades |  |  |
| C4.17 | Would NELFT Service Desk be expected to provide support after go live | To what capacity |  |
| C4.18 | Who will be expected to train NELFT users | Please state where training will be held | After initial training, what training support will be given going forward |
| C4.19 | How would future NELFT employees be trained |  |  |
| C4.20 | Has this software been deployed to any other NHS trust | Please list maximum of 3 other trust | Trust contact details |

## C5 - Interoperability criteria

Establishing how well your product exchanges data with other systems.

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 an appropriate clinical system without being restricted to one type. Those technologies that need to interface within clinical record systems must also be interoperable. Application Programme Interfaces (API’s) should follow the Government Digital Services Open API Best Practices, be documented and freely available and third parties should have reasonable access in order to integrate technologies.

Good interoperability reduces expenditure, complexity and delivery times on local system integration projects by standardising technology and interface specifications and simplifying integration. It allows it to be replicated and scaled up and opens the market for innovation by defining the standards to develop to upfront.

This section should be tailored to the specific use case of the product and the needs of the buyer however it should reflect the standards used within the NHS and social care and also direction of travel.

Please provide details relating to the specific technology and not generally to your organisation.

|  |  |  |
| --- | --- | --- |
| **Code** | **Question** | **Supporting Answer** |
| C5.1 | Does your product expose any Application Program Interfaces (API) or integration channels for other consumers? | Yes | No |
| C5.1.1 | If yes, please provide detail and evidence:   * The API’s (e.g. what they connect to) * Set out the healthcare standards of data interoperability eg. 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. | Free text |
| C5.2 | Do you use NHS number to identify patient record data? | Yes | No | No because product doesn’t identify patient record data |
| C5.2.1 | 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. | Free text |
| C5.3 | 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) | Yes | No | No because the product doesn’t read/ write into EHRs |
| C5.3.1 | If yes, please detail the standard | Free text |
| C5.3.2 | If no, please state the reasons and mitigations, methodology and security measures. | Free text |
| C5.4 | Is your product a wearable or device, or does it integrate with them? | Yes | No |
| C5.4.1 | If yes, provide evidence of how it complies with ISO/IEEE 11073 Personal Health Data (PHD) Standards. | Attached | No evidence available |

# 

# 

# Please upload relevant supporting documentation

Please ensure documents are clearly labelled with the name of your company, the question number and the date of submission. Any documents incorrectly labelled will be rejected at triage stage.

Possible documents to be attached are:

* A11 - CQC Report
* B4 - User journeys and data flows
* C1.1.1 - Clinical Risk Management System
* C1.1.2 - Clinical Safety Case Report
* C1.1.2 - Hazard Log
* C1.3.2 - UK Medical Device Regulations 2002 Declaration of Conformity and if applicable Certificate of Conformity
* C1.4.1 - Clinical Risk Management documentation and Conformity certificate for third party suppliers
* C2.1 - Information Commissioner's registration or completed Self-assessment Outcome Tool
* C2.2.1 Completed Information Commissioner’s Self-assessment Outcome Tool
* C2.3.2 - Data Protection Impact Assessment (DPIA)
* C3.1 - Cyber Essentials Certification
* C3.2 - External Penetration Test Summary Report
* C4.4.1 - If a wearable, evidence of how the product complies with ISO/IEEE 11073 Personal Health Data (PHD) Standards