Public – To be published on the Trust external website

Digital Technology Assessment Criteria (DTAC)

Ref: IT-0037-v1

Status: Approved
Document type: Procedure
Overarching Policy: N/A

Contents

1 Introduction

Digital Technology Assessment Criteria (DTAC) is a process for identifying and minimising the risks associated with supply chain. It is for use with new suppliers and should also be utilised with existing suppliers who may not have previously completed a DTAC assessment at the discretion of the Trust. This procedure formalises current Trust practice.

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

Our Journey To Change sets out why we do what we do, the kind of organisation we want to become and the way we will get there by living our values, all of the time. To achieve this, the Trust has committed to three goals. This procedure supports all three goals of Our Journey To Change.

Goals 1 (To co-create a great experience for patients, carers, and families) and 2 (To co-create a great experience for our colleagues): 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. Implementing this procedure provides assurance to patients, careers, families, and staff that when systems and processes are introduced or changed, their privacy, data security and clinical safety has been considered from the outset.

Goal 3 (To be a great partner): The DTAC brings together legislation and good practice in these areas. It is the national baseline criteria for digital health technologies entering and already used in the NHS and social care. Information and its governance is a key communication tool and is strategic in assisting the Trust when it works with key partners either to improve services or to jointly care for patients. When we tell our patients who we work with and have robust agreements about what is going to be shared we enable information to support outstanding care and service delivery with our partners.

2 Purpose

All new digital technology should be assessed using the DTAC, whether it be in pilot/trial or procured/adopted for full implementation. If multiple products are to be considered, each one would require a DTAC.

Examples of products include: staff facing and patient facing digital health tech, health apps, medical devices and devices with an associated app, systems, web based portals and any IT enabled technology across the Trust. Following this procedure will ensure the Trust:-

- Meets its legal obligations in carrying out an assessment of the impact of the envisaged processing operations on the protection of personal data in support of the Data Protection Impact Assessment (DPIA) process.
- Ensures that good cyber hygiene is being followed and/or remediated should any gaps in process or systems be highlighted as part of this process.
- Helps to improve supply chain transparency and build strong foundational relationships.
- Complies with standard DCB0160 mandated under Health and Social Care Act 2012 ensuring all Health IT has been risk assessed in order to minimise potential patient harm

3 Scope

3.1 What this procedure applies to

- This procedure is to be followed when introducing a new digital technology, whether it be in pilot/trial or procured/adopted for full implementation.

The assessment criteria is focused on 5 core areas. Sections 1 to 4 form the assessed criteria, with a separate conformity rating provided around usability and accessibility which is assessed as part of overall procurement:

A DTAC new supplier assessment will be sent to new suppliers for completion as part of standard procurement process.

1. **Clinical safety**
Products are assessed to ensure that clinical safety measures are in place and that organisations undertake clinical risk management activities to manage this risk.

In order for the Trust to procure a product which impacts or influences direct patient care. Products or systems must comply with the Health and social care act 2012 by having DCB0160 Accreditation.

Examples of products or systems that must comply with DCB0160, Electronic Patient Record systems, Digital Medical devices, IT systems supporting patient treatment such as CBT, Diagnostic tools, Telehealth. CCTV, bodycams and other recording devices

Examples of products or systems that do not need to comply with DCB0160
Health rostering, business systems or systems which only exist for research and development systems

The Trust has an existing Clinical Safety Case process which pre-dates DTAC and will continue to be used as it meets requirement. The Trust may on occasion sub contract out clinical safety cases or reviews of existing cases. Clinical Safety case procedure link

Please direct any specific enquiries to: CSO.enquiries@nhs.net

2. Data protection
Products are assessed to ensure that data protection and privacy is 'by design' and the rights of individuals are protected.

The Trust has an existing Data Protection Impact Assessment (DPIA) process which pre-dates DTAC and will continue to be used as it meets requirement. DPIA procedure link

Please direct any specific enquiries to: TEWV.DPIA@nhs.net

3. Technical assurance
Products are assessed to ensure that products are secure and stable.

The Trust requires that the DTAC technical elements V1 2023 form is completed. Please see Appendix 3.

4. Interoperability
Products are assessed to ensure that data is communicated accurately and quickly whilst staying safe and secure.

The Trust assess interoperability as part of DTAC technical elements V1 2023 form is completed. Please see Appendix 3.

Please direct any specific enquiries to: TEWV.cyber@nhs.net

5. Usability and accessibility
Products are allocated a conformity rating having been benchmarked against good practice and the NHS service standard.

The DTAC includes company information and value proposition sections for context. Each of the scored and assessed sections contain:

- a reference code for each question
- the question for the developer to respond to
- whether evidence is required or not
- supporting information and guidance
- scoring criteria

Usability and accessibility will be assessed as part of the procurement specification for new procurements. Please direct any specific enquiries to: TEAWVNT.ITprocurement@nhs.net

3.2 Who this procedure applies to

This procedure applies to all new suppliers and can be retrospectively used for existing suppliers as and when required.

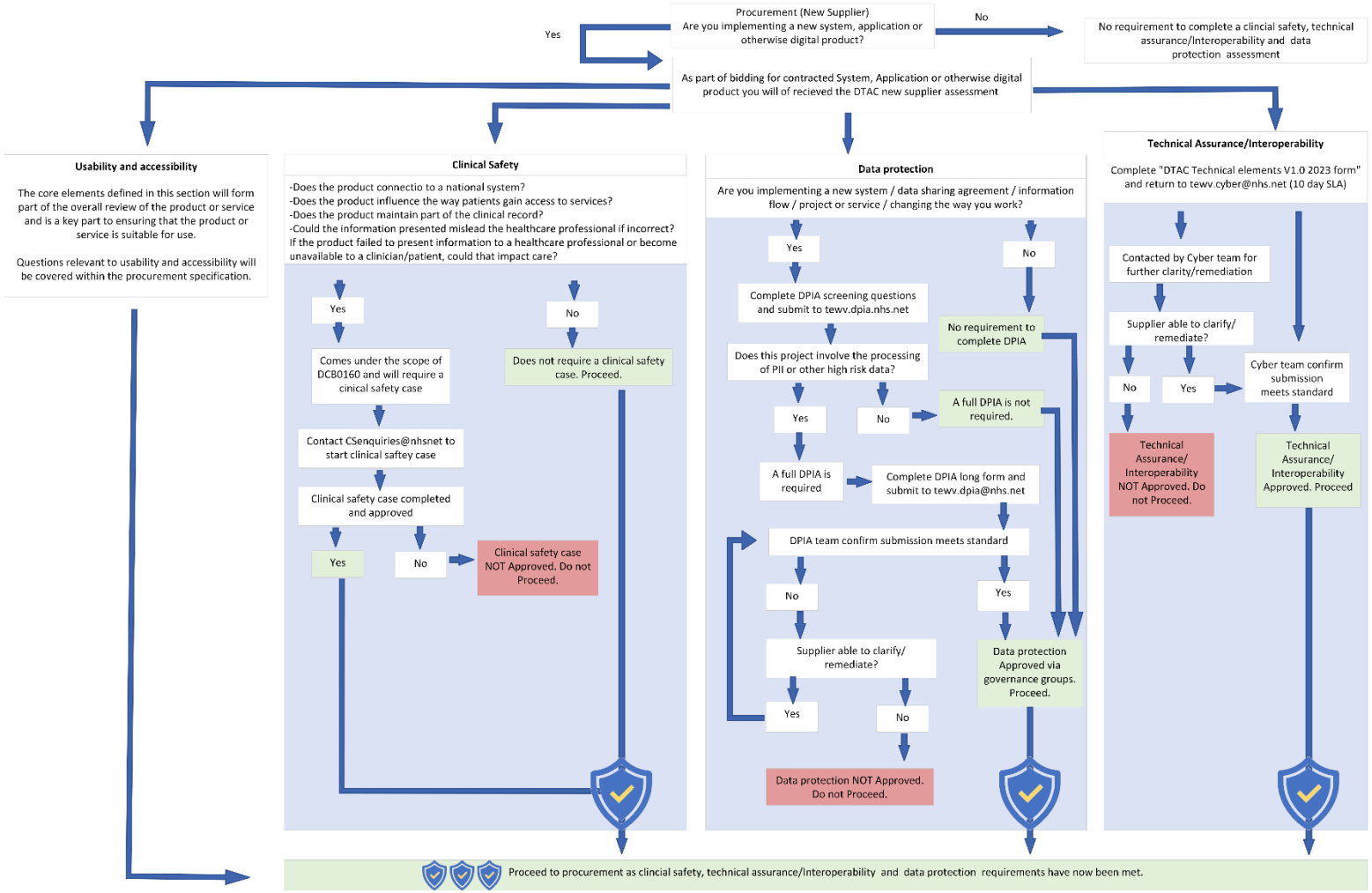
It is the Information Asset Owner (IAO) responsibility for ensuring DTAC is completed. DTAC is a live process which is to be maintained for the lifecycle of the system which must be reviewed annually and/or when changes to process are proposed.

4 Related documents

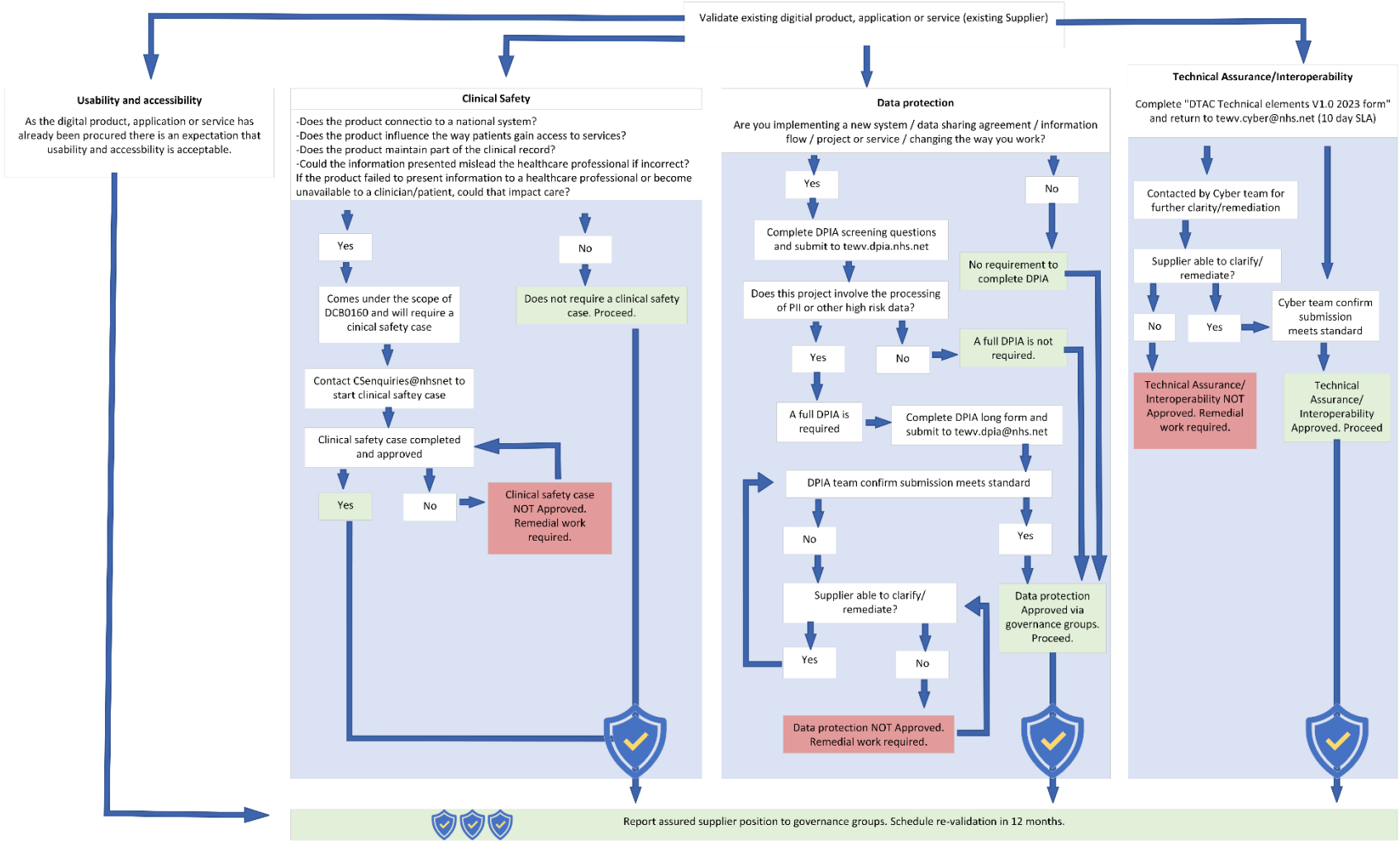
This procedure also refers to:-

- Maintenance of IT Systems Policy
- Introduction or Upgrade of Information Systems Procedure
- Trust Project and Programme Management Frameworks (P3M framework)
- DPIA procedure
- Digital and Data Contract Management Policy
- Clinical Risk Management Procedure
- Organisational Risk Management Policy

5 Process flow New procurements (see appendix 4 for accessible version)



6 Process flow - existing digital products, applications or services (see appendix 5 for accessible version)



6.1 Identify the need for a DTAC assessment

All new digital technology should be assessed using the DTAC, whether it be in pilot/trial or procured/adopted for full implementation. If multiple products are to be considered, each one would require a DTAC.

Existing systems already under contract or otherwise in use within the Trust will be scheduled to undergo a retrospective DTAC which follows the same process aside from moving onto procurement as the product or service will already be procured. Retrospective DTAC assessments will be carried out at the discretion of the Trust based on risk.

6.2 Where do I obtain a DTAC assessment form?

- For New Digital systems, products or services being procured all required forms will be sent as part of the Trusts procurement process.
- For existing systems a DTAC pack will be sent to the supplier directly and responses will be validated as per the process flow within this document.

6.3 Completing the DTAC form

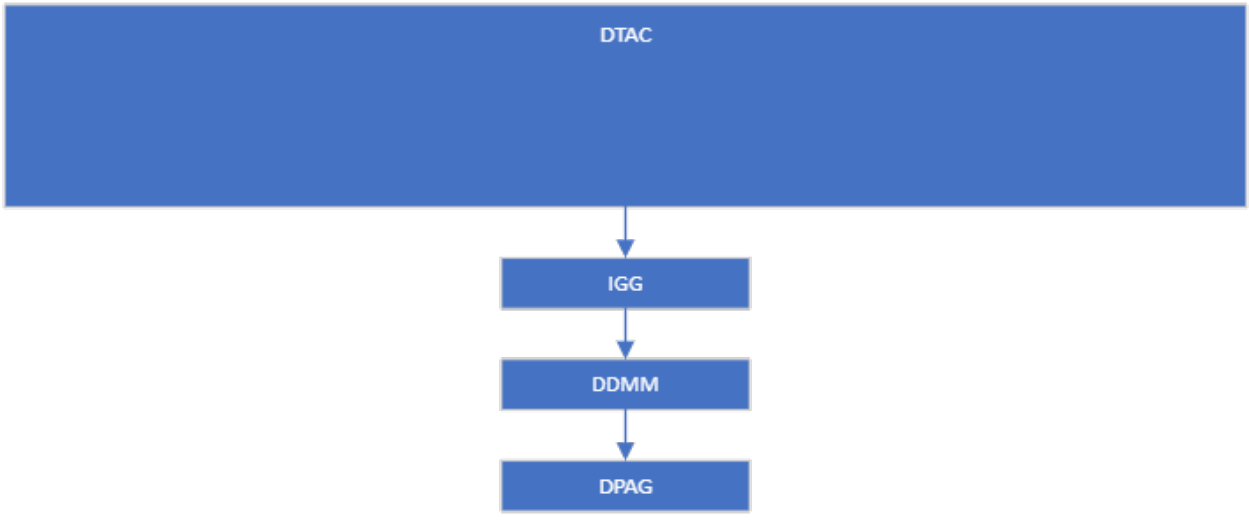
DTAC is self-explanatory and includes instructions for completion and pass/fail criteria.

For specific support or queries please contact the responsible lead:

- Data protection: TEWV.DPIA@nhs.net
- Clinical Safety: CSO.enquiries@nhs.net
- Technical assurance / Interoperability: TEWV.cyber@nhs.net
- Usability and accessibility - Procurement: TEAWVNT.ITprocurement@nhs.net

6.4 Quality Assurance and Approval

The 5 principles of each DTAC will be discussed and ratified for approval at Information Governance Group (IGG)/Digital & Data Management Meeting (DDMM) and for approval at Digital Performance and Assurance Group (DPAG) with notification to be sent to DPB if delays to project delivery are incurred.



Residual risks may have follow-on actions following project closure and require monitoring. Those that remain will be logged on the Trust's risk management system and a risk manager and owner assigned – see Organisational Risk Management Policy for the Trust approach to managing risk.

Following Approval at DPAG, the Clinical Safety Case, DPIA and Technical assurance/Intermobility will be maintained throughout the life of the product until decommissioning and reviewed annually.

6.5 Mitigating and managing risks

Any high risks highlighted through DTAC must be escalated to the DPAG for final approval or before any processing takes place. Any residual high risks that cannot be mitigated must be reported to the Information Commissioners Office (ICO). Please contact tewv.ig@nhs.net for further advice.

Any residual project risks will be recorded and managed via the project's Risks, Assumptions, Issues and Decisions (RAID) log.

Residual risks may have follow-on actions following project closure and require monitoring. Those that remain will be logged on the Trust's risk management system and a risk manager and owner assigned – see Organisational Risk Management Policy for the Trust approach to managing risk.

7 Terms and definitions

Term	Definition
CCTV	Closed circuit television
Bodycam	A small wearable video camera to increase transparency and trust
Telehealth	Telehealth is the use of digital information and communication technologies to access health care services remotely and manage your health care
CBT	Cognitive behavioural therapy

8 How this procedure will be implemented

- This procedure will be published on the Trust's intranet and external website.
- Line managers will disseminate this procedure to all Trust employees through a line management briefing.

8.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
All staff	IG training	90 minutes	Annual

9 How the implementation of this procedure will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	DTAC Pass Fail Criteria (as set out in national DTAC form provided by NHS England)	F = for each DTAC assessment M = as per process flows set out in this document (Section 5 & 6). R = as set out in the above flow charts.	DDMM/IGG/DPAG

10 References

https://transform.england.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac/

11 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	30 January 2024
Next review date	30 January 2027
This document replaces	n/a – new document
This document was approved by	Digital and Data Management Meeting
This document was approved	30 January 2024

This document was ratified by	n/a
This document was ratified	n/a
An equality analysis was completed on this policy on	03/07/2023
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
1	30 Jan 2024	New document	Approved

Appendix 1 - Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Digital and Data Services
Title	DTAC Procedure
Type	Procedure/guidance
Geographical area covered	Trust-wide
Aims and objectives	This procedure aims to ensure that all new digital technology is assessed for risk using the DTAC, whether it be in pilot/trial or procured/adopted for full implementation.
Start date of Equality Analysis Screening	01 March 2023
End date of Equality Analysis Screening	26 June 2023

Section 2	Impacts
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	Staff, patients and their carers and families
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual, Heterosexual, Pansexual and Asexual etc.) **NO**

	• **Age** (includes, young people, older people – people of all ages) **NO** • **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed Forces** (includes serving armed forces personnel, reservists, veterans and their families) **NO**
Describe any negative impacts	None identified
Describe any positive impacts	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. Implementing this procedure provides assurance to patients, careers, families, and staff that when systems and processes are introduced or changed, their privacy, data security and clinical safety has been considered from the outset. The DTAC brings together legislation and good practice in these areas. It is the national baseline criteria for digital health technologies entering and already used in the NHS and social care. Information and its governance is a key communication tool and is strategic in assisting the Trust when it works with key partners either to improve services or to jointly care for patients. When we tell our patients who we work with and have robust agreements about what is going to be shared we enable information to support outstanding care and service delivery with our partners.

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	Data Protection Act 2018 Health and Social Care Act 2012 NHS England best practice guidance

Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes - Trustwide staff consultation conducted
If you answered Yes above, describe the engagement and involvement that has taken place	Note - Clinical safety cases are written with the involvement of patients, carers and their families. The Clinical Risk Management Procedure and the DPIA Procedure which form parts of the DTAC have undergone Trust-wide consultation.
If you answered No above, describe future plans that you may have to engage and involve people from different groups	

Section 4	**Training needs**
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	n/a
Describe any training needs for patients	n/a
Describe any training needs for contractors or other outside agencies	n/a

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 2 – Approval checklist

To be completed by lead and attached to any document which guides practice when submitted to the appropriate committee/group for consideration and approval.

	Title of document being reviewed:	Yes / No / Not applicable	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Y	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Y	
2.	**Rationale**		
	Are reasons for development of the document stated?	Y	
3.	**Development Process**		
	Are people involved in the development identified?	Y	
	Has relevant expertise has been sought/used?	Y	
	Is there evidence of consultation with stakeholders and users?	Y	trustwide consultation
	Have any related documents or documents that are impacted by this change been identified and updated?	n/a	
4.	**Content**		
	Is the objective of the document clear?	Y	
	Is the target population clear and unambiguous?	Y	
	Are the intended outcomes described?	Y	
	Are the statements clear and unambiguous?	Y	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	y	NHS England DTAC best practice
	Are key references cited?	Y	
	Are supporting documents referenced?	Y	
6.	**Training**		
	Have training needs been considered?	Y	
	Are training needs included in the document?	Y	

	Title of document being reviewed:	Yes / No / Not applicable	Comments
7.	**Implementation and monitoring**		
	Does the document identify how it will be implemented and monitored?	Y	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Y	
	Have Equality and Diversity reviewed and approved the equality analysis?	Y	Approved by E&D 28/06/2023
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Y	
10.	**Publication**		
	Has the policy been reviewed for harm?	yes	No harm
	Does the document identify whether it is private or public?	yes	Public
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	n/a	

Appendix 3 – DTAC technical elements V1 2023

TEWV NHS Foundation Trust

Digital Technology Assessment Criteria (DTAC) - Compliance with Relevant information Security Standards and Protocols – Technical Security & Interoperability

Standard	***Response*** ***Yes/No***	*Scoring criteria*
Technical security - Cyber essentials/Cyber essentials Plus		To pass, developers must have a valid Cyber Essentials certificate. Certification lasts for a period of 12 months so the certificate should be within date. This should be validated against the IASME database. NHS organisations are required to have Cyber Essentials in place (and is now incorporated into the NHS Digital Data Security and Protection Toolkit (DSPT) for NHS Trusts and Foundation Trusts in 2021-22 assessments) and to mitigate risk within the supply chain, **suppliers must hold Cyber Essentials and preferably cyber essentials plus.**
Technical Security - ISO 27001		Does the supplier hold a valid ISO 27001 certification. Details of current certificate held to be provided and a copy of the certificate.
Technical security - Please confirm whether all custom code had a security review.		To pass, the developer must confirm that an internal or an external custom code security review has been undertaken. An external review is preferable; however an internal code review would meet the baseline requirement. The supplier should be performing static and dynamic code review. Evidence to be supplied of how internal code reviews are undertaken.
Has the system/software supplied been penetration tested or vulnerability assessed within the last 12 months?		Please provide appropriate evidence. The Trust will sign an NDA to ensure any sensitive findings are not shared with any other party. It is expected that any highlighted risks have an appropriated remediation plan.
Technical security - Please confirm whether all privileged accounts have appropriate Multi-Factor Authentication (MFA)?		To pass, the developer must confirm yes that all privileged accounts have MFA employed. The supplier should have the capability to employ MFA on all user accounts accessing the system from January 2023.
Technical security - Please confirm whether logging and reporting requirements have been clearly defined.		To pass, the developer must confirm yes that logging and reporting requirements have been clearly defined. Please detail your current logging and reporting systems/mechanisms and if a SIEM/SOC is employed within the environment.
Technical security - Please confirm whether the product has been load tested		To pass, the developer must confirm yes that load testing has been performed and provide evidence of testing.

Interoperability (C4.1) - Does your product expose any Application Programme Interfaces (API) or integration channels for other consumers?		To pass, developers must demonstrate that they have API's that are relevant to the use case for the product, follow Government Digital Services Open API Best Practice, are documented and freely available and that third parties have reasonable access to connect. APIs should adopt generally accepted standards of data interoperability for the NHS or social care dependent on the use case for the product. If the product does not have API's and there is a legitimate rationale for this considering the use case of the product then the buyer can accept this rationale.
Interoperability (C4.1.1) If yes to C4.1, 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.		See above.
Interoperability (C4.3) Does your product have the capability for		To pass, developers should confirm that the product has the capability to read/write into EHRs using industry standards for secure interoperability.

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. (C4.3.1) If no and applicable, please detail any mitigation and security measures taken. (4.3.2.)		If a product does not use industry standards, then a legitimate rationale should be set out and the security, usability and appropriateness of the methodology should be considered. If yes, please detail the standard. If no, state the reasons and mitigations, methodology and security measures.
Interoperability (C4.4) Is your product a wearable or device, or does it integrate with them?		To pass, the developer must evidence compliance with ISO/IEEE 10073
Interoperability (C4.4.1) If yes, provide evidence of how it complies with ISO/IEEE 11073 Personal Health Data (PHD) Standards.		
Is your product classified as a medical device. If answering Yes, what is its intended function.		Provide details of intended function as a medical device and classification. Medical devices: how to comply with the legal requirements in Great Britain - GOV.UK (www.gov.uk)

Appendix 4 - DTAC process flow new procurements (accessible text version)

Purpose

Validate Procurement (New Supplier) for new system, application or otherwise digital product

(if procurement is for none of the above then there is no requirement to complete a clinical safety, technical assurance/Interoperability and data protection assessment)

What domains are assessed?

As part of bidding for contracted System, Application or otherwise digital product you will of received the DTAC new supplier assessment. This tests four domains.

All four domain requirements must be met. The four domains are:-

Usability and accessibility
Clinical Safety
Data protection
Technical Assurance/Interoperability

Domain: Usability and accessibility

The core elements defined in this section will form part of the overall review of the product or service and is a key part to ensuring that the product or service is suitable for use.

Questions relevant to usability and accessibility will be covered within the procurement specification.

The product or service must meet the procurement specification for the domain requirement to be met.

Domain: Clinical Safety

-Does the product connect to a national system?
-Does the product influence the way patients gain access to services?
-Does the product maintain part of the clinical record?
-Could the information presented mislead the healthcare professional if incorrect?
-If the product failed to present information to a healthcare professional or become unavailable to a clinician/patient, could that impact care?

If yes to any of the above, a Clinicals Safety Case must be completed and approved before this domain requirement is met.

If no to all of the above, then Clinical Safety case is not needed and this domain requirement is met.

Domain: Data protection

Are you implementing a new system / data sharing agreement / information flow / project or service / changing the way you work?

If yes to any of these the full DPIA process must be followed. The DPIA is assessed by the DPIA team, If assessment by DPIA Team finds issue that the supplier fails to clarify or remediate as required then the DPIA not approved – and procurement must not proceed. If DPIA approved by DPIA Team the proceed to approval via governance groups to for this domain requirement to be met.

If no to all, then Data protection is approved by via governance groups and the domain requirement is met.

Domain: Technical Assurance/Interoperability

Action for supplier: Complete "DTAC Technical elements V1.0 2023 form" and return to tewv.cyber@nhs.net (10 day SLA)

Cyber Team: reviews the completed form, requests any required clarifications/ remediation, then if all conditions are met confirms submission meets standard. This confirmation indicates this domain requirement is met.

Are requirements of all four domains met?

If all four domains:-

Usability and accessibility

Clinical Safety

Data protection

Technical Assurance/Interoperability

are assured, then proceed to procurement as clinical safety, technical assurance/Interoperability and data protection requirements have now been met.

Appendix 5 – DTAC process flow for existing products (accessible text version)

Purpose

Validate existing digital product, application or service (existing Supplier)

What domains are assessed?

All four domain requirements must be met. The four domains are:-

Usability and accessibility
Clinical Safety
Data protection
Technical Assurance/Interoperability

Domain: Usability and accessibility

As the digital product, application or service has already been procured there is an expectation that usability and accessibility is acceptable. The domain requirement automatically met by default.

Domain: Clinical Safety

-Does the product connect to a national system?
-Does the product influence the way patients gain access to services?
-Does the product maintain part of the clinical record?
-Could the information presented mislead the healthcare professional if incorrect?
-If the product failed to present information to a healthcare professional or become unavailable to a clinician/patient, could that impact care?

If yes to any of the above, a Clinicals Safety Case must be completed and approved before this domain requirement is met.
If no to all of the above, then no Clinical Safety case is needed and this domain requirement is met.

Domain: Data protection

Are you implementing a new system / data sharing agreement / information flow / project or service / changing the way you work?

If yes to any of these the fully DPIA process must be followed and approved to for this domain requirement to be met.

If no to all, then the domain requirement is met.

Domain: Technical Assurance/Interoperability

Action for supplier: Complete "DTAC Technical elements V1.0 2023 form" and return to tewv.cyber@nhs.net (10 day SLA)

Cyber Team: reviews the completed form, requests any required clarifications/ remediation, then if all conditions are met grants approval. This approval indicates this domain requirement is met.

Are requirements of all four domains met?

If all four domains:-

Usability and accessibility
Clinical Safety
Data protection
Technical Assurance/Interoperability

are assured, then report assured supplier position to governance groups. Schedule re-validation in 12 months.