

Data Protection Impact Assessment Form



1) Basic Information about New / Change of System / Project

Completed by – Title(s):	
Description of subject of assessment:	
Asset / System Name:	
Executive Sponsor – Title:	
Project Manager – Title:	
Information Asset Owner – Title:	
Information Asset Administrator - Title:	



2) Key Questions

Question		Response	Comment
2.1	Will the system / process / change (now referred to as 'asset') involve the use of personal identifiable data or confidential data?	Yes / No	
2.2	State the purpose for the processing of the data.		
2.3	Does the asset involve new privacy invasive technology (including but not limited to biometrics, facial recognition decision making algorithms)?	Yes / No If Yes – provide details	
2.4	Does the asset involve collecting new personal data not previously collected?	Yes / No	
2.5	Has the asset been recorded within Corestream – the Trust electronic Information Asset Register?	Yes / No	
2.6	Does the asset involve contacting individuals in ways they may feel are unnecessarily intrusive?	Yes / No	
2.7	Does the asset involve using existing information in a different way?	Yes / No	

Question		Response	Comment
2.8	Please select personal data that will be collected:	☐ Personal details (e.g. name, address, contact details, age, gender, race, physical description, NHS no, NI no.)	
		☐ Family circumstances (i.e. marital status, housing, travel, leisure activities, membership of charities)	
		☐ Education and training details (i.e. qualifications, skills database, training records)	
		☐ Employment details (i.e. career history, recruitment and termination details, attendance records, appraisals, health and safety records, security records)	
		☐ Financial details (i.e. income, salary, investments)	

Question		Response	Comment
		☐ Goods or services provided (i.e. details of services provided, licences issued, contracts, agreements)	
		☐ Racial or ethnic origin	
		☐ Political opinions	
		☐ Religious & other beliefs	
		☐ Trade Union Member	
		☐ Physical or mental health condition	
		☐ Sexual life	
		☐ Offences (including alleged)	
		☐ Criminal Proceedings	
2.9	What steps have been taken to ensure that the collection of confidential and / or sensitive data is relevant and necessary?	Please provide details in comment section.	

Question		Response	Comment
2.9a	Will this processing actually help to achieve the stated purpose?	Yes / No	
2.9b	Is the processing proportionate to that purpose?	Yes / No Please provide details in comment section.	
2.9c	Can the same purpose be achieved without the processing?	Yes / No Please provide details in comment section.	
2.9d	Can the same purpose be achieved by processing less data, or by processing the data in another more obvious or less intrusive way?	Yes / No Please provide details in comment section.	
2.10	Will the information collected be passed onto other parties who have not previously received it?	Yes / No	
2.11	Are new or changed data collection policies involved that may be intrusive or unclear?	Yes / No	
2.12	Is the asset supplied by a 3 rd party? If Yes, are they registered with the Information Commissioner?	Yes / No Yes / No If Yes – provide their DPA Notification Number:	

Question		Response	Comment
2.13	DCB 0129 / DCB 0160 completion Has the manufacturer of the IT system completed a DCB 0129? Has the healthcare organisation implementing the system completed a DCB 160?	Yes / No / Not applicable Yes / No / Not applicable	
2.14	Digital Technology Assessment Criteria for Health and Social Care (DTAC) Will the product be used to provide electronic information for health or social care purposes? <i>Example: The procurement of a new clinical system (Cleric)</i> The DTAC is completed by the <i>supplier</i> through the Procurement process but will require clinical and IT collaboration <i>as part of each new procurement process or contract renewal.</i>	Yes / No / Not applicable If yes, then please complete a DTAC assessment form	 DTAC_version_1.0_FI NAL_updated_16.04.c
2.15	Has a SECamb Supplier Security Assessment form been completed? This form is provided by the Head of Information Security & Business Continuity.	Yes / No / Not applicable If yes, please provide a copy.	

Question		Response	Comment
2.16	Does the process involve the use of AI? If yes, then a separate AI DPIA will need to be completed.	Yes / No	
2.17	Does the 3rd party contract contain the required Information Governance clauses including Data Protection and Freedom of Information?	Yes / No If Yes – provide details in comments section:	
2.18	Does the asset comply with Privacy and Electronic Regulations 2003? The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the UK GDPR. They give people specific privacy rights in relation to electronic communications. There are specific rules on: • marketing calls, emails, texts and faxes; • cookies (and similar technologies); • keeping communications services secure; and • customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.	Yes / No / Not applicable	
2.19	Who provides information for the asset?	Give details in comments section:	
2.20	What is the legal basis for processing of personal or sensitive data?	Give details in comments section:	

Question		Response	Comment
	(Data protection legislation) Relevant UK GDPR Articles must be illustrated	Where consent is the legal basis provide details of how the consent will be obtained and recorded.	
2.21	Have individuals given consent to data processing and disclosures, where required? (Common Law Duty of Confidentiality)	☐ Yes (explicit) Give details of how the consent has been obtained and recorded. ☐ Yes (implicit) Give details of how this processing meets the “reasonable expectations” of a data subject ☐ No If No – give details in comments section of those specifically withdrawn:	
2.22	If data is to be processed without consent, where is this recorded?	☐ Information Asset Register ☐ Data Flow ☐ Caldicott Approval ☐ Other – Provide details	

Question		Response	Comment
2.23	How will the accuracy and completeness of information in the asset be maintained?	Provide details in comments section:	
2.24	Who will have access to information in the asset, and what security measures will be in place?	Provide details in comments section. Include details of audit trail facilities to be included:	
2.25	Can the data subject request access to their data	Yes / No If Yes – provide details on this process in the comments section:	
2.26	Can the data subject request that their data is rectified or forgotten?	Yes / No If Yes – provide details on the process to be followed, and how it is to be communicated, in the comments section :	
2.27	Does the asset involve changing the medium that publicly available information is distributed?	Yes / No If Yes – provide details in the comments section:	
2.28	Where will information in the asset be stored?	Provide details in the comments section:	
2.29	How will the information in the asset be accessed?	Provide details in the comments section:	

Question		Response	Comment
2.30	What is the data retention period for data in the asset?	Provide details in the comments section:	
2.31	How will data in the asset be destroyed at the end of the retention period?	Provide details in the comments section:	
2.32	Does the asset involve sending information off site?	Yes / No If Yes – Provide details of where it is being sent in the comments section: If Yes – Provide details of the method of transport to be used: If Yes – will any personal or sensitive data be transferred outside the European Economic Area? Provide details of what data will be sent, and where:	
2.33	Is the intention for the data controller to seek the views of data subjects (or their representatives) related to the purpose and means of the processing operation?	Yes / No If Yes – provide details in the comments section on the method of gathering these views.	

Question		Response	Comment
		Provide details of the views received back from the data subject. Provide details of the final decision to go ahead with the proposed change, or not, based upon the views received from the data subjects. If No – Provide reasons in the comments section of the justification for not seeking the views of the data subjects.	

Section 2.13 – Reference Information

DCB 0129 and DCB 0160 are two standards issued by NHS Digital.

DCB 0129 applies to the manufacturers of health IT systems whereas DCB 0160 applies to the healthcare organisations implementing them.

They require manufacturers of health IT systems and healthcare organisations to carry out a particular type of risk assessment on the product. This process determines whether the product is acceptably safe to go live. The requirements in the two standards are almost identical.

The organisation must:

1. Nominate a clinical safety officer
2. Define and document clinical risk management processes
3. Carry out a risk assessment and document that in a Hazard Log and Safety Case
4. Conduct clinical risk management activities during live service to keep the safety case up to date

Section 2.14 The Digital Technology Assessment Criteria for health and social care (DTAC)

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 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 intention is to smooth the path between development and procurement so that the NHS and social care may realise the benefits that digital technologies can bring. Assurance is confirmed through completion and ratification of a DTAC assessment form.

This is completed by the *supplier through the Procurement process but will require clinical and IT collaboration* as part of each *new procurement process or contract renewal*. Buyers of digital health technology should ask the developer to complete the DTAC by responding to the question set and providing the evidence required.

Whilst the DTAC is intended to be a common baseline criterion in terms of safety and security, it is intended to be one part of procurement - it is not intended to be the complete question set for procurements and should be supplemented with additional specifications including any policy and regulatory requirements.

3) Cloud Service Considerations

This section requires completing if a 'Cloud' based solution is involved.

Question		Response	Comment
3.1	Why is a cloud-based solution being considered over an in-house solution?	Provide details in comments section:	
3.2	What type of data will be hosted in the cloud?	Provide details in comments section:	
3.3	Will the cloud service be hosted on the Health and Social Care Network (HSCN) network?	Provide details in comments section:	
3.4	What measures have been put in place in the event of the service provider ceasing to operate?	Provide details in comments section:	
3.5	Has an assessment of the cloud service providers financial position and solvency been performed?	Provide details in comments section:	

3.6	What measures have been put in place to repatriate data from the asset in the cloud service back to the Trust, at the end of the service contract?	Provide details in comments section, including any additional infrastructure requirements and associated costs to the Trust:	
3.7	Has the legal team been consulted regarding the legal ownership of any data that is uploaded to the asset in the cloud service?	Provide details in comments section:	
3.8	What security measures are in place for the asset in the cloud service, including protection from cyber security attacks, control of user access to the data, secure transfer of data between the cloud service provider and the Trust?	Provide details in comments and provide a copy of SECamb Supplier Security Assessment:	

4) **Data Flow**

This section describes the data owners and processors, and the flow of data between them.

5) Risk Management

An essential element of the DPIA process is the assessment of risks, and identification of actions that will mitigate the risk from occurring or make the situation acceptable if the risk materialised. Record any new risks identified from performing the DPIA here.

Description	Consequence on the data subject of the risk occurring (1-5)	Likelihood of the risk occurring (1-5)	Score	Is the risk Accepted or Mitigated – give details	Consequence following mitigation (1-5)	Likelihood following mitigation (1-5)	Score

6) References

List any policies, procedures, guidance or legislation referred to within the DPIA here:

7) Record of Approval

Document Status:	
DPIA Status:	Approved / Rejected
Comments:	

Information Governance Lead Approval:	
Name:	
Title:	
Signature:	
Date:	

Data Protection Officer Approval:	
Name:	
Signature:	
Date:	

<u>SIRO Approval:</u>	
Name:	
Title:	
Signature:	
Date:	

<u>IAO Approval:</u>	
Name:	
Title:	
Signature:	
Date:	

Please return the completed DPIA form to:
Information.governance@secamb.nhs.uk