



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	
2.4	Does the asset involve collecting new personal data not previously collected?	Yes/No	
2.5	Does the asset involve contacting individuals in ways they may feel are unnecessarily intrusive?	Yes/No	
2.6	Does the asset involve using existing information in a different way?	Yes/No	
2.7	Please select personal data that will be collected:	<input type="checkbox"/> Personal details (e.g. name, address, contact details, age, gender, race, physical description, NHS no, NI no.)	



		<input type="checkbox"/> Family circumstances (i.e. marital status, housing, travel, leisure activities, membership of charities)	
		<input type="checkbox"/> Education and training details (i.e. qualifications, skills database, training records)	
		<input type="checkbox"/> Employment details (i.e. career history, recruitment and termination details, attendance records, appraisals, health and safety records, security records)	
		<input type="checkbox"/> Financial details (i.e. income, salary, investments)	
		<input type="checkbox"/> Goods or services provided (i.e. details of services provided, licences issued, contracts, agreements)	
		<input type="checkbox"/> Racial or ethnic origin	
		<input type="checkbox"/> Political opinions	
		<input type="checkbox"/> Religious & other beliefs	



		<input type="checkbox"/> Trade Union Member	
		<input type="checkbox"/> Physical or mental health condition	
		<input type="checkbox"/> Sexual life	
		<input type="checkbox"/> Offences (including alleged)	
		<input type="checkbox"/> Criminal Proceedings	
2.8	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.	
2.8a	Will this processing actually help to achieve the stated purpose?	Yes/No Please provide details in comment section.	
2.8b	Is the processing proportionate to that purpose?	Yes/No Please provide details in comment section.	
2.8c	Can the same purpose be achieved without the processing?	Yes/No Please provide details in comment section.	
2.8d	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.	



2.9	Will the information collected be passed onto other parties who have not previously received it?	Yes/No If Yes – give details	
2.10	Are new or changed data collection policies involved that may be intrusive or unclear?	Yes/No If Yes – give details	
2.11	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:	
2.11a	Does the 3 rd party contract contain the required Information Governance clauses including Data Protection and Freedom of Information?	Yes/No If Yes – provide details in comments section:	
2.12	Does the asset comply with Privacy and Electronic Regulations 2003?	Yes/No	
2.13	Who provides information for the asset?	Give details in comments section:	
2.14	What is the legal basis for processing of personal or sensitive data? (Data protection legislation) Relevant GDPR Articles must be illustrated	Give details in comments section: Where consent is the legal basis provide details of how the consent will be obtained and recorded.	



2.15	Have individuals given consent to data processing and disclosures, where required? (Common Law Duty of Confidentiality)	<input type="checkbox"/> Yes (explicit) Give details of how the consent has been obtained and recorded. <input type="checkbox"/> Yes (implicit) Give details of how this processing meets the “reasonable expectations” of a data subject <input type="checkbox"/> No If No – give details in comments section of those specifically withdrawn:	
2.16	If data is to be processed without consent, where is this recorded?	<input type="checkbox"/> Information Asset Register <input type="checkbox"/> Data Flow <input type="checkbox"/> Caldicott Approval <input type="checkbox"/> Other – Provide details	
2.17	How will the accuracy and completeness of information in the asset be maintained?	Provide details in comments section:	



2.18	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:	
2.19	Can the data subject request access to their data	Yes/No If Yes – provide details on this process in the comments section:	
2.20	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 :	
2.21	Does the asset involve changing the medium that publicly available information is distributed?	Yes/No If Yes – provide details in the comments section:	
2.22	Where will information in the asset be stored?	Provide details in the comments section:	
2.23	How will the information in the asset be accessed?	Provide details in the comments section:	
2.24	What is the data retention period for data in the asset?	Provide details in the comments section:	
2.25	How will data in the asset be destroyed at the end of the retention period?	Provide details in the comments section:	



2.26	Does the asset involve sending information off site?	<p>Yes/No</p> <p>If Yes – Provide details of where it is being sent in the comments section:</p> <p>If Yes – Provide details of the method of transport to be used:</p> <p>If Yes – will any personal or sensitive data be transferred outside the European Economic Area?</p> <p>Provide details of what data will be sent, and where:</p>	
2.27	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?	<p>Yes/No</p> <p>If Yes – provide details in the comments section on the method of gathering these views.</p> <p>Provide details of the views received back from the data subject.</p> <p>Provide details of the final decision to go ahead with the</p>	



		<p>proposed change, or not, based upon the views received from the data subjects.</p> <p>If No – Provide reasons in the comments section of the justification for not seeking the views of the data subjects.</p>	
--	--	---	--

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 N3 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 section:	



4) Data Flow

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

Architecture overview will be attached



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.

Datix ID	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
	Could send information to the wrong person. Small reputational risk if this were to occur but unlikely to contain any information which translates to being personally identifiable. Will only occur if a telephone number is provided incorrectly or if a telephone changes hands.							
	Could inappropriately send out confidential information regarding patients to users. This would potentially be a data breach however in all likelihood it would be data that the individuals who would be receiving the alert would be exposed to through normal operations and therefore of no consequence. Good practices are already enforced around messaging and no IWR-1s have							



	been received in at least a year where this has occurred.							

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 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