



DATA PROTECTION IMPACT ASSESSMENT

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

This DPIA template must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that uses personal data.

Template Version 1.0 July 2022

Document Version Control

Version	Reason	Date	Author(s)

Project / Work Stream Name:		
Project / Work Stream Lead: <i>(Who is leading the project or implementation)</i>	Name:	
	Designation:	
	Email:	
Information Asset Owner: <i>(Who will be responsible for the data that is stored / created)</i>	Name:	
	Designation:	
	Email:	
Key Stakeholder Names and Roles:		
Overview: <i>(Summary of the project/work stream)</i>		
Timeframe for the project / work stream: <i>(When is it due to begin? If time limited, when does it end / need to be reviewed)</i>		
Environmental Scan: <i>Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.</i>		



Step 1: Complete the Screening Questions

Q	Category	Screening question	Check if Yes
1.1	Technology	Does the project introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy?	<input type="checkbox"/>
1.2	Technology	Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business?	<input type="checkbox"/>
1.3	Identity	Does the project involve new identifiers, re-use or existing identifiers e.g. NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data?	<input type="checkbox"/>
1.4	Identity	Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?	<input type="checkbox"/>
1.5	Multiple organisations	Does the project involve multiple organisations, whether they are public sector agencies i.e. joined up government initiatives or private sector organisations e.g. outsourced service providers or business partners?	<input type="checkbox"/>
1.6	Data	Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled?	<input type="checkbox"/>
1.7	Data	Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database?	<input type="checkbox"/>
1.8	Data	Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals?	<input type="checkbox"/>
1.9	Data	Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources?	<input type="checkbox"/>
1.10	Data	Will the personal data be processed out of the UK?	<input type="checkbox"/>
1.11	Exemptions and Exceptions	Does the project relate to data processing which is in any way exempt from legislative privacy protections?	<input type="checkbox"/>



Q	Category	Screening question	Check if Yes
1.12	Exemptions and Exceptions	Does the project's justification include significant contributions to public security and measures?	<input type="checkbox"/>
1.13	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	<input type="checkbox"/>

The purpose of the screening questions is to confirm that the data protection laws are being complied with, or highlights problems that need to be addressed. It also aims to prevent problems arising at a later stage which might impede the progress or success of the project.

Answering "Yes" to any of the screening questions above represents a potential Information Governance (IG) risk factor, please proceed and complete the next section.



Step 2: Identify the need for a DPIA						
2.1	Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared?				New	<input type="checkbox"/>
					Changed	<input type="checkbox"/>
2.2	Please specify data used. For items marked "*" please provide more detail in the box. If forms or data definitions are available, please include					
	Personal Data					
	Name	<input type="checkbox"/>	Address	<input type="checkbox"/>	Postcode	<input type="checkbox"/>
	Email	<input type="checkbox"/>	Phone / Mobile	<input type="checkbox"/>	Date of Birth	<input type="checkbox"/>
	NHS No. / EPR ID No.	<input type="checkbox"/>	NI No.	<input type="checkbox"/>	Payroll number	<input type="checkbox"/>
	Driving licence	<input type="checkbox"/>	Bank / Credit details	<input type="checkbox"/>	Tax / Benefit / Pension	<input type="checkbox"/>
	School Records	<input type="checkbox"/>	Housing Records	<input type="checkbox"/>	Other identifiers* (e.g. mother's maiden name, passwords, logins)	<input type="checkbox"/>
	Special Category Personal Data					
	Racial / ethnic origin	<input type="checkbox"/>	Political Opinions	<input type="checkbox"/>	Religious or philosophical beliefs	<input type="checkbox"/>
	Trade Union Membership	<input type="checkbox"/>	Physical or mental health*	<input type="checkbox"/>	Sexual life*	<input type="checkbox"/>
	Criminal offences*	<input type="checkbox"/>	Biometrics* (DNA profile, fingerprints, etc.)	<input type="checkbox"/>	Adoption records*	<input type="checkbox"/>
	Social services records*	<input type="checkbox"/>	Child protection records*	<input type="checkbox"/>	Safeguarding records*	<input type="checkbox"/>
	Other personally identifiable data (please list)					
	Further details of items marked *					
2.3	Business sensitive data	Check if Yes	Details			
	Financial	<input type="checkbox"/>				
	Local Contract conditions	<input type="checkbox"/>				
	Operational data	<input type="checkbox"/>				



	Notes associated with patentable inventions	<input type="checkbox"/>	
	Procurement/tendering information	<input type="checkbox"/>	
	Customer/supplier information	<input type="checkbox"/>	
	Decisions impacting:	One or more business functions	<input type="checkbox"/>
		Across the organisation	<input type="checkbox"/>
	Description of other business data processed/shared/viewed (if any).		



Step 3: Describe the sharing/processing							
3.1	List of organisations/partners involved in sharing or processing personal/special categories personal data.						
	<i>If more rows are needed, select the right-hand box in the last row and click "+".</i>						
	Name or class of organisation	Type of Organisation (drop-down)	Completed and compliant with the Data Security and Protection (DSP) Toolkit (drop-down)				
		Choose an item.	Choose an item.				
3.2	Is there an existing 'Data Processing Contract' or 'Data Sharing Agreement' between the Controller and the Processor? <i>If no, please provide details of legal route for Article 26/28 compliance below</i>			Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
3.3	Has a data flow mapping exercise been undertaken? <i>If yes, please provide a copy at Annex 2 below, if no, please provide clear reason why not in the box below.</i>			Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
3.4	Does the project involve employing contractors external to the Organisation who would have access to personal or special categories of personal data? Please check if Yes. <i>If checked, provide a copy of the confidentiality agreement or contract as an annex</i>					<input type="checkbox"/>	
3.5	Describe in as much detail why this information is being processed/shared/viewed? <i>(For example Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use)</i>						



Step 4: Assess necessity and proportionality

4.1 Lawfulness for Processing/sharing personal data/special categories of personal data?
You need to check one box in each section. For most health and care purposes, it's the first box in each section.

Personally Identifiable Data	
<input type="checkbox"/>	<p>The DPA section 8(c) – “the exercise of a function conferred on a person by an enactment or rule of law”, specifically the NHS Act 2006 and the Health and Social Care Act 2012, allowing use of UK GDPR Article 6(1)(e) ‘...for the performance of a task carried out in the public interest or in the exercise of official authority...’</p> <p>Note: This is the most common legal basis for health and care processing</p>
<input type="checkbox"/>	<p>UK GDPR Article 6(1)(a) – “the data subject has given consent to the processing of his or her personal data for one or more specific purposes;”</p> <p>Note: This is a very rare and unusual case in health and care. Relying on this has legal consequences which need to be reviewed elsewhere in the DPIA.</p>
<input type="checkbox"/>	<p>UK GDPR Article 6(1)(b) – “...for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;”</p> <p>Note: The DATA SUBJECT must be part of the contract; we cannot rely on this basis for contracts between health bodies.</p>
<input type="checkbox"/>	<p>UK GDPR Article 6(1)(c) – “...for compliance with a legal obligation to which the controller is subject;”</p> <p>Note: There is no need to check this one if one of the above is checked.</p>
<input type="checkbox"/>	<p>UK GDPR Article 6(1)(d) – “...in order to protect the vital interests of the data subject or of another natural person;”</p> <p>Note: There is no need to check this one if one of the above is checked.</p>
<input type="checkbox"/>	<p>UK GDPR Article 6(1)(f) – “...for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;”</p> <p>Note: Public authorities cannot rely on legitimate interest. If you are using this, there needs to be careful review to ensure that you are not formally a public authority.</p>
Special Categories of Personally Identifiable Data	
<input type="checkbox"/>	<p>The DPA section 10(1)(c) – health and social care via Schedule 1 Part 1 section 2 “Health or social care purposes” satisfying DPA section 10 (2) allowing use of UK GDPR Article 9(2)(h) ‘...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...’</p> <p>Note: This is the most common legal basis for health and care processing</p>



	<input type="checkbox"/>	<p>UK GDPR Article 9(2)(a) – “the data subject has given explicit consent to the processing of those personal data for one or more specified purposes...”</p> <p>Note: This is a very rare and unusual case in Health and care. Relying on this has legal consequences which need to be reviewed elsewhere in the DPIA.</p>
	<input type="checkbox"/>	<p>DPA Section 10(2) meeting a criterion in Part 1 of schedule 1 allowing use of UK GDPR Article 9(2)(b) – “...necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law ...”</p> <p>Note: This generally would apply staff or patients in social care situations not covered by DPA Section 10. There is no need to check this one if DPA Section 10(1)(c) above is checked.</p>
		<p>If you checked this section, detail below which criterion in Part 1 of Schedule 1 is met?</p>
	<input type="checkbox"/>	<p>UK GDPR Article 9(2)(c) – “...necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;”</p> <p>Note: There is no need to check this one if DPA Section 10(1)(c) above is checked.</p>
	<input type="checkbox"/>	<p>UK GDPR Article 9(2)(d) – “...carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim...”</p> <p>Note: This is unlikely for health and care bodies.</p>
	<input type="checkbox"/>	<p>UK GDPR Article 9(2)(e) – “...relates to personal data which are manifestly made public by the data subject;”</p> <p>Note: This is unusual and would only apply in rare circumstances. Note that this excludes data made public by someone <i>other</i> than the data subject.</p>
	<input type="checkbox"/>	<p>UK GDPR Article 9(2)(f) – “...necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;”</p> <p>Note: There is no need to check this one if DPA Section 10(1)(c) above is checked.</p>
	<input type="checkbox"/>	<p>DPA Section 10(1)(b) “substantial public interest” satisfying a condition in DPA Schedule 1 Part 2, allowing use of UK GDPR Article 9(2)(g) “...necessary for reasons of substantial public interest...”</p> <p>Note: There is no need to check this one if DPA Section 10(1)(c) above is checked.</p>
		<p>If you checked this section, detail below which criterion in Part 2 of Schedule 1 is met?</p>



	<input type="checkbox"/>	DPA Section 10(1)(d) “public health”, satisfying Section 3 of DPA Schedule 1 Part 1, allowing use of UK GDPR Article 9(2)(i) – “...necessary for reasons of public interest in the area of public health...” Note: This is very distinct from the health and care purpose 10(1)(c). It is possible, but uncommon, to have processing that is in both areas.		
	<input type="checkbox"/>	DPA Section 10(1)(e) “archiving, research and statistics”, satisfying Section 4 of DPA Schedule 1 Part 1, allowing use of UK GDPR Article 9(2)(j) – “necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes ...” Note: Most statistics are covered by health and care processing, this is most commonly used for approved medical research, the National Archive or non-medical statistics involving personal data.		
	If you checked this section, detail below how the requirements of DPA Section 19 and Article 89 UK GDPR are met?			
4.2	Will the information be processed/shared electronically, on paper or both?	Electronic	<input type="checkbox"/>	
		Paper	<input type="checkbox"/>	
4.3	How will you ensure data quality and data minimisation? <i>Note that if existing processes cover the rights, please answer “Existing Processes”. The reviewer may confirm these processes.</i>			
4.4	Have individuals been informed about the proposed use of their personal or special categories of personal data? If No, how is the transparency principle met? <i>For example, do the organisations/partners listed in section 3.1 have updated Fair Processing Notice available to patients on their websites?</i>	Yes	<input type="checkbox"/>	
		No	<input type="checkbox"/>	
4.5	How will you recognise and respond to rights requests from individuals? <i>Note that if existing processes cover the rights, please answer “Existing Processes”. The reviewer may confirm these processes.</i> <i>Note that ALL rights must be covered, not just subject access.</i>			
4.6	How will you recognise and respond to data breaches? <i>Note that if existing processes cover the right, please answer “Existing Processes”. The reviewer may confirm these processes.</i>			
4.7	Will the processing of data include automated individual decision-making, including profiling?	Yes	<input type="checkbox"/>	



	<i>If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject</i>	No	<input type="checkbox"/>
4.8	If Consent is used as the legal basis above, how will consent be obtained and recorded? <i>If not using consent, respond N/A</i>		
4.9	As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so please complete the cloud security questionnaire and add as an annex or state below why it is not required. <i>Note that the questionnaire is not required for systems that already have a separate DPIA.</i>	Yes	<input type="checkbox"/>
		No	<input type="checkbox"/>
4.10	Where will the data will be stored? <i>Please state countries of storage, locations and types used. Examples of Storage include bespoke system, e.g. EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet, storage area/filing room and location, etc.</i>		
4.11	Data Retention Period <i>How long will the data be kept?</i>		
4.12	Will this information being shared/processed outside the organisations listed above in question 3? <i>If yes, describe who and why:</i>	Yes	<input type="checkbox"/>
		No	<input type="checkbox"/>
4.13	Is there linking of information between different data sets? <i>If yes, describe how this is achieved and the legal basis for doing so. Note that linking data where patients are not clients of both organisations needs particular review.</i>	Yes	<input type="checkbox"/>
		No	<input type="checkbox"/>



Step 5: Information Security Process				
5.1	Is there an ability to audit access to the information? <i>If no, please provide a reason why this is not required. If yes, please describe auditing.</i>	Yes	<input type="checkbox"/>	
		No	<input type="checkbox"/>	
5.2	How will access to information be controlled?			
5.3	What roles will have access to the information? (list individuals or staff groups)			
5.4	What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?			
	Username and password	<input type="checkbox"/>	Smartcard <input type="checkbox"/> key to locked filing cabinet/room <input type="checkbox"/>	
	Secure 1x Token Access including authenticator apps, SMS	<input type="checkbox"/>	Restricted access to Network Files <input type="checkbox"/>	
	Other: <i>Provide a Description Below:</i>			
5.5	Is there a documented System Level Security Policy (SLSP) for this project? If yes, please add a copy as an annex. SLSP is required for new systems. <i>SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.</i>	Yes	<input type="checkbox"/>	
		No	<input type="checkbox"/>	
		Not a new system	<input type="checkbox"/>	
5.6	Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process? <i>Please explain and give reference to such plan and protocol</i>	Yes	<input type="checkbox"/>	
		No	<input type="checkbox"/>	
		Not a new system	<input type="checkbox"/>	
5.7	Is Mandatory Staff Training in place for the following?	Yes	No	N/A
	Data Collection, where there is new data being collected?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



	Use of the System or Service, for new systems?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Information Governance, where organisations involved are not toolkit certified?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	If you answered any of the above as "Yes" or "No" please detail training <i>A response is not needed if all answers were N/A</i>				
5.8	Are there any new or additional reporting requirements for this project? <i>If no, skip to 5.9. If yes, provide details below.</i>	Yes		<input type="checkbox"/>	
		No		<input type="checkbox"/>	
	What roles will be able to run reports?				
	What roles will receive the report or where will it be published?				
	Will the reports be in person-identifiable, pseudonymised or anonymised/aggregate format?				
	Identifiable	<input type="checkbox"/>	Pseudonymised	<input type="checkbox"/>	Anonymised/Aggregate
Will the reports be in business sensitive or redacted format (removing anything which is sensitive)?					
Business Sensitive	<input type="checkbox"/>	Business Redacted	<input type="checkbox"/>	No Business Data	<input type="checkbox"/>



Step 6: Identify and Assess Risks

Note that this section should only cover risks of the NEW or CHANGED process. If existing systems are used, their protective measures are covered in the DPIA / SLSP for the system and should not be repeated here.

Risk Scoring

Score	Likelihood of Harm (L)	Severity of Harm (S)
1	Rare – can't believe this will ever happen	Insignificant – no injury or adverse outcome; no risk to persons or organisation. Unlikely to cause complaint. Litigation risk remote
2	Unlikely – do not expect to happen, but possible	Minor – short term injury / damage; minimal risk to persons or organisation. Complaint possible, litigation possible.
3	Occasionally - May occur	Moderate – semi-permanent injury / damage risk to persons or organisation. Complaint likely; litigation possible, but not certain
4	Likely – will probably occur but it is not a persistent issue	Major – risks of severe injury / damage to persons or organisation. Litigation expected/certain. Local adverse publicity.
5	Almost certain – likely to occur on many occasions, a persistent issue	Catastrophic – risk of death or inability of organisation to continue. Formal investigation likely, litigation certain, national adverse publicity.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. <i>If you need more rows, click in the last box on the right of the last row, then click the “+”.</i>	Likelihood of harm (L)	Severity of harm (S)	Overall risk (L x S)
	Choose an item.	Choose an item.	Choose an item.



Step 7: Identify Measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 6

If you need more rows, click in the last box on the right of the last row, then click the “+”.

Risk	Options to reduce risk likelihood or severity	Effect on risk	Residual risk (see above for scores)			Measure approved
			L	S	Score	
		Choose an item.				Choose an item.



Step 8: Sign off and record outcomes

Item	Details		Notes
IG Subgroup Reviewed	Date:		Please note here subgroup comments or revisions.
Risk Measures approved by:	Name:		
	Role:		
	Date:		
Residual risks accepted by:	Name:		Must be a SIRO, IAO or Caldicott Guardian
	Role:		
	Date:		

DPO Advice section – Each Controller to Complete, duplicate this section as needed.

Controller:			
DPO advice provided by:	Name:		
	Date:		
Summary of DPO advice:			
DPO advice accepted or overruled by:	Name:		If overruled, you must explain your reasons in explanation, below.
	Role:		
	Date:		
Explanation:			
<i>End of DPO Advice Section</i>			



Item	Details		Notes
Consultation responses reviewed by:	Name:		If your decision departs from individuals' views, you must explain your reasons below.
	Role:		
	Date:		
Explanation:			
The DPIA will be reviewed by the respective DPOs / IAOs of each organisation when required.			



ANNEX 1. GLOSSARY OF TERMS

Anonymised Data - means data in a form where the identity of the individual cannot be recognised i.e. when: Reference to any data item that could lead to an individual being identified has been removed; The data cannot be combined with any other data sources to produce personal identifiable data.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Flow Mapping (DFM) means the process of documenting the flows/transfers of Personal Data, Sensitive Personal Data (known as special categories personal data under UK GDPR) and Commercially Confidential Information from one location to another and the method by which they flow.

Data Subject – an individual who is the subject of personal information or can be identified from it.

Direct Care - means clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care. (National Data Guardian definition)

EPR means electronic patient record system; these are the primary systems which provide access to patient

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Special Categories of Personal Data mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.



ANNEX 2. DATA FLOW DIAGRAM

TBA

