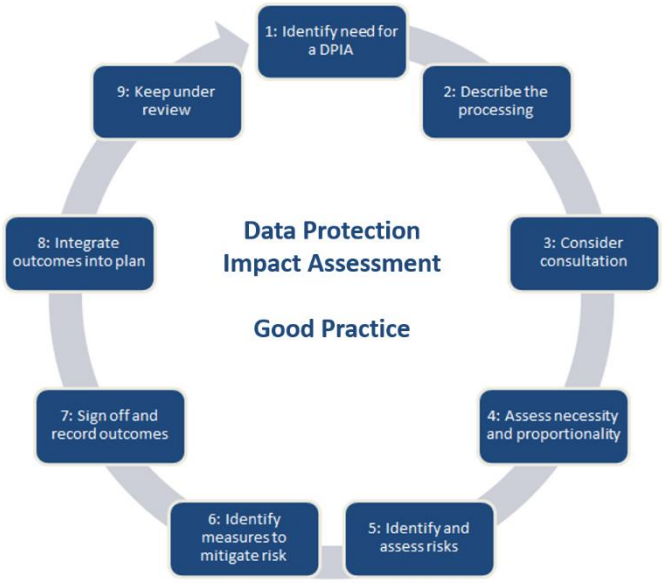
5 Coles Lane, Oakington, UK, Cambridge, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org

OPC DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project. DPIA must be complete at the start of any project involving the use of Personal Data, or if you are making a significant change to an existing Company process.

The final outcomes of the DPIA should be signed off by the OPC Senior Information Risk Owner or Data Protection Officer (DPO) or appropriate delegate and integrated back into the project plan or process documentation.

Before completing the DPIA, please use the DPIA Screening Checklist below to help decide if a DPIA is required for a project or for data access. Please seek advice from the OPC Data Protection Officer (DPO) about when to do a DPIA.



DPIA SCREENING CHECKLIST

CHECKLIST	RESPONSE (YES/NO)	DPIA REQUIREMENT
Does the project involve the use of personal data?		If YES – DPIA required
Does the project involve processing of personal data that could result in a risk of physical harm in the event of a security breach		If YES – DPIA required
Does the project involve processing of sensitive data or data of a highly personal nature?		If YES – DPIA required
Does the project require processing of data concerning vulnerable data subjects		If YES – DPIA required
Does the project use systematic and extensive profiling or automated decision-making to make significant decisions about people?		If YES – DPIA required
Does the project involved processing on a large scale (e.g. regional or national)		If YES – DPIA required
Does the project require processing of pseudonymised data with no reasonable risk of re-identification?		If YES – DPIA not required but should be considered
Does the project require processing of pseudonymised data with reasonable risk of re-identification e.g. processing at site?		If YES – DPIA required
Does the project involve only anonymised record level data at small scale (e.g. 100,000 data subjects or less)?		If YES – DPIA not required
Does the project involve only anonymised record level data at small scale (e.g. more than 100,000 data subjects)?		If YES – DPIA not required but should be considered
Does the project involve only anonymised and aggregated data?		Yes – DPIA not required
Does the project combine, compare or match data from multiple sources?		Yes – DPIA required

5 Coles Lane, Oakington, UK, Cambridge, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org

DATA PROTECTION IMPACT ASSESSMENT FORM

SUBMITTING ORGANISATION DETAILS	
Project Name:	
Submitting Organisation:	
Organisation contact (name, job title, email, phone):	
DPIA Submission Date:	

IDENTIFY THE NEED FOR A DPIA
Explain broadly what project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA. *You may find it helpful to refer or link to other documents, such as a project proposal.*

5 Coles Lane, Oakington, UK, Cambridge, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org

DESCRIBE THE PROCESSING

Describe the nature of the processing: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: What is the nature of the data, and does it include any patient identifiable information? How much data will be collected and/or used (e.g. number of data subjects)? How long will you keep the data?

5 Coles Lane, Oakington, UK, Cambridge, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org

Describe the context of the processing: Would data subjects expect their data to be used in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security concerns? Is it novel in any way or common industry practice? Are there any current issues of public concern you should factor in?

Describe the purposes and benefits of the processing: What do you want to achieve by processing the data? What are the benefits of the processing – directly and indirectly or more broadly?

5 Coles Lane, Oakington, UK, Cambridge, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org

CONSULTATION PROCESS
Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. This may include other members in your organisation, DPOs, data processors, or any other experts?

DATA PROTECTION COMPLIANCE AND PROPORTIONALITY – must be assessed by OPC DPO
Describe compliance with data protection principles under GDPR and lawful basis for processing. Include measures for proportionality i.e. data minimisation: What is the lawful basis for processing? How will you ensure data security, data quality and data minimisation? What information will you give data subjects and how will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

5 Coles Lane, Oakington, UK, Cambridge, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org

IDENTIFY AND ASSESS RISKS

Describe source of risk and nature of potential impact on data subjects.

RISK	**Likelihood of harm** Remote, Possible or Probable	**Severity of harm** Minimal, Significant or Severe	**Overall risk** Low, Medium or High

IDENTIFY MEASURES TO REDUCE OR MITIGATE RISKS

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk and state any residual risk.

RISK	**Measures to reduce or eliminate risk**	**Effect on risk** Eliminated, Reduced or Accepted	**Measure approved** Yes or No

5 Coles Lane, Oakington, UK, Cambridge, CB24 3BA
T: 01223 967855 E: info@optimumpatientcare.org

DPIA OUTCOMES AND SIGN OFF		
Item	**Name/position/date**	**Notes**
Risk mitigation measures approved by:		*Measures should be recorded in project plan or suitable documentation*
Residual risks identified approved by:		*Residual risk must be assessed by DPO to assess if ICO consult if required*
DPO advice provided by:		*DPO should advise on data protection compliance and whether processing can proceed*
Summary of DPO advice:		
DPIA Outcome (Decision Reached):		
Next DPIA review date:		*DPO should review ongoing compliance with DPIA*
On behalf of Optimum patient Care (OPC), this data protection impact assessment is approved		
Signature:		
Name:		
Position:		
Date:		