

Short Form DPIA

This template is used to record a Data Protection Impact Assessment (DPIA) for data processes determined to be low risk following a risk assessment.

It follows the process set out in the ICO DPIA guidance, and should be read alongside that guidance and the [criteria for an acceptable DPIA](#) set out in European guidelines on DPIAs.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Key Documents Provided to BCHC for this Assessment

Privacy Notice	Yes / No
Data Protection/GDPR Policy	Yes / No
Information Security Policy	Yes / No
IT Security Policy	Yes / No
Online GDPR/DPA statement	Yes / No
Working SOPs/manuals	Yes / No please state which ones
DSPT certification	Yes / No
Cyber Essentials certification	Yes / No
ISO certification	Yes / No
Any other accreditation certifications	Yes / No please state which ones
Assessments, audit, internal testing documents	Yes / No please state which ones
BCHC's information security assessment	Yes / No please state which ones
Any other documents not listed above	please state which ones

Step 1: 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 based on the Risk Assessment.

1. Summary of project

a.

2. Need for DPIA

a. (Record Risk Assessment Selections and Outcome)

Step 2: 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?

[enter flow diagram here]

1. How is the data collected and processed?
2. What personal data is involved?
3. How is the data stored?
4. Is the data shared with anyone?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

1. Nature of the data collected?
2. What individuals are affected?
3. How is the data being stored?
4. Where is the data stored (location)?
5. How is the data secured?
6. What is the retention period for the data and justification for retaining it for this period?
7. How will the data be destroyed following the retention period?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

1. What is the wider context of the processing?
2. Are there prior concerns over this type of processing or security flaws?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

1. What are the benefits to patients or staff of the intended processing?
2. What are the benefits to the Trust of undertaking the processing?
3. Could the same benefits be achieved without processing personal data?

Step 3: 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. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

1. Is a third party processor or application involved in this activity?
2. Is the data accessible to anyone else?
3. Is there a data sharing agreement in place with the third party? If not why not?
4. Is it necessary to seek a view from the ICO as to the proposed processing activity? If not, why not?
5. Which Trust officers have been involved in this assessment?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

1. What is the lawful basis for processing?
2. How does the processing actually achieve your purpose (proportionality and necessity of processing)?
3. How will you ensure data quality, data minimization and restricted access to data?
4. How will individuals be informed as to their data being processed?
5. What risks will there be to the data subjects from processing of their data?
6. How will the activity support data subject's rights?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Severity of harm	Likelihood of harm	Overall risk

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk (Eliminated, reduced, accepted)	Residual risk (Low, medium, high)	Measure approved (Yes, No)

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, measures to reduce risk and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA