Kingsmead Healthcare

Responsibility, Trust, Compassion

Data Protection Impact Assessment (DPIA) Protocol

Introduction

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.

We must do a DPIA for processing that is **likely to result in a high risk** to individuals. This includes some specified types of processing.

It is also good practice to do a DPIA for any other major project which requires the processing of personal data.

A DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

In assessing the level of risk, we must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

We should consult our data protection officer and, where appropriate, individuals and relevant experts.

DPIA Awareness checklist

We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

Our existing policies, processes and procedures include references to DPIA requirements.

We understand the types of processing that require a DPIA and use the screening checklist to identify the need for a DPIA, where necessary.

We have created and documented a DPIA process.

We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist

Consider carrying out a DPIA in any major project involving the use of personal data.

Consider whether to do a DPIA if we plan to carry out any other:

evaluation or scoring;

automated decision-making with significant effects;

systematic monitoring;

processing of sensitive data or data of a highly personal nature;

processing on a large scale;

processing of data concerning vulnerable data subjects;

innovative technological or organisational solutions;

processing that involves preventing data subjects from exercising a right or using a service or contract.

We always carry out a DPIA if we plan to:

- use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- process special-category data or criminal-offence data on a large scale;
- systematically monitor a publicly accessible place on a large scale;
- use innovative technology in combination with any of the criteria in the European guidelines;
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- carry out profiling on a large scale;
- process biometric or genetic data in combination with any of the criteria in the European guidelines;
- combine, compare or match data from multiple sources; process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
- process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
- process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
- process personal data that could result in a risk of physical harm in the event of a security breach.
- We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.
- If we decide not to carry out a DPIA, we document our reasons.

DPIA process checklist

- We describe the nature, scope, context and purposes of the processing.

- We ask our data processors to help us understand and document their processing activities and identify any associated risks.
- We consider how best to consult individuals (or their representatives) and other relevant stakeholders.
- We ask for the advice of our data protection officer.
- We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure compliance with data protection principles.
- We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.
- We identify measures we can put in place to eliminate or reduce high risks.
- We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.
- We implement the measures we identified, and integrate them into our project plan.
- We consult the ICO before processing, if we cannot mitigate high risks.
- We keep our DPIAs under review and revisit them when necessary.

Have we written a good DPIA?

A good DPIA helps you to evidence that:

- you have considered the risks related to your intended processing; and
- you have met your broader data protection obligations.

This checklist will help ensure you have written a good DPIA.

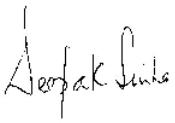
We have:

- confirmed whether the DPIA is a review of pre-GDPR processing or covers intended processing, including timelines in either case;

Kingsmead Healthcare

Responsibility, Trust, Compassion

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Name	Dr Jamal ARSHAD Information Governance Lead	Deepak Sinha General Manager
Signature		
Approval Date	01.04.2022	
Review Date	31.03.2023	