**Data Protection Impact Assessment (DPIA) Template**

**Introduction**

A data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. Once completed, the DPIA should be emailed to Data Security & Protection Team: [dhcft.datasecurityandprotection@nhs.net](mailto:dhcft.datasecurityandprotection@nhs.net)

The General Data Protection Regulations (GDPR) introduces a new obligation to do a DPIA before carrying out types of processing likely to result in high risk to individuals’ interests. If your DPIA identifies a high risk that you cannot mitigate, the DPO will consult with the Information Commissioner’s Office.

A DPIA does not have to eradicate the risks altogether, but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability and building trust and engagement with individuals.

**When do I need to complete a DPIA?**

You must do a DPIA before you begin any type of processing which is “likely to result in a high risk”. This means that although you have not yet assessed the actual level of risk you need to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, a DPIA must be completed if you plan to:

* process special category (including health) or criminal offence data on a large scale; or
* use new technologies;
* use profiling or special category data to decide on access to services;
* match data or combine datasets from different sources;
* collect personal data from a source other than the individual without providing them with a privacy notice (‘invisible processing’);
* track individuals’ location or behaviour;
* profile children or target marketing or online services at them; or
* process data that might endanger the individual’s physical health or safety in the event of a security breach.

If you are unsure whether to complete a DPIA please ask the IG Team to advise.

**Who completes the DPIA?**

The project or service lead should complete the template. Advice can be sought from the Data Security & Protection Team: [dhcft.datasecurityandprotection@nhs.net](mailto:dhcft.datasecurityandprotection@nhs.net)

**DPIA Template** – complete all sections and send to [dhcft.datasecurityandprotection@nhs.net](mailto:dhcft.datasecurityandprotection@nhs.net)

|  |  |
| --- | --- |
| Name: |  |
| Job Title: |  |
| Email address and telephone number: |  |
| Title of project being assessed: |  |
|  | |
| **Brief description of the aim / desired outcome / purpose of the project**: | |
|  | |
| **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 another way of describing data flows. | |
|  | |
| **Describe the scope of the processing:** what is the nature of the data, and does it include special category (e.g. health) 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? | |
|  | |
| **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? | |
|  | |
| **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? | |
|  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | |  |  |  |
| **Identify and assess risks (please include Fraud Risk):** | | | |  |  |  |
| **Describe the source of risk and nature of potential impact on individuals.**  Include associated compliance and corporate risks as necessary. | **Likelihood of harm**  (Remote, Possible or Probable) | **Severity of harm**  (Minimal, Significant or Severe) | **Overall risk**  (Low, Medium or High) | **Action(s) to reduce or eliminate the risk** | **Risk level after mitigation** | **Outcome i.e. mitigation to be implemented or risk accepted.** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Sign Off and Outcomes**

|  |  |  |
| --- | --- | --- |
| **Item** | **Name / Date** | **Notes** |
| **Risk mitigation measures approved by:** |  | Integrate actions back in to project plan, with date and responsibility for completion. |
| **Residual risks approved by:** |  | If accepting any residual high risk, consult the ICO before going ahead. |
| **Data Protection Officer (DPO) advice given by:** |  | DPO should advise on compliance, risks assessed and whether processing can proceed. |
| **Record of Processing Activity (ROPA)** | Has Asset register and data flow mapping updated accordingly?  Have Information Asset Owner / Admin been assigned?  Is it relevant to refer to Change Advisory Group (CAB) for change control and also Clinical Digital Practice for clinical safety case?  Is it relevant for Cyber Essential and ISO 27001 / 02 certification? |  |
| **Summary of DPO advice:** | | |
|  | | |
| **DPO advice accepted or overruled by:** |  | If overruled, you must explain your reasons in the comments below. |
| **Comments:** | | |
|  | | |