Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our 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.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
• The Outpatient Antimicrobial Chemotherapy Patient Management System (OPAT PMS) is a nationally used and recognized software solution to aid in the treatment and management of patients on OPAT. The software is owned and managed by Horizon Strategic Partners (HSP). • The system collects special category data in the form of health-related personal data. As an example, this covers, demographic, past and current medical history. We are required to produce a DPIA due to the capture of special category data. • In addition to the above we collect the name, and email address of the Data Controller.

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?*

- The data is collected by the User (data controller) who is a medical professional and is then entered into the system manually via a selection of input fields.
- Data is stored within an encrypted server that is only accessible via the N3 network.
- Data can be deleted via the user from within the system or upon request to HSP. This addresses the requirement with the right to be forgotten.
- Data is hosted with a third party, this is stated in the product contract which is signed by the Data Controller in order to use the product.
- Data is not shared with any third party organizations.
- Data is not used or accessed unless requested by the User (data controller). This helps limit risk when accessing data. A log of each access is stored.
- Aggregate reports are generated by the system, for User's use only. These aggregate reports can be shared with other medical organizations, only if the user agrees.
- Data Controllers name, and email address are used for product updates and support of the system.

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?*

- HSP does not use any data of any kind, other than email addresses of the data controllers who access the system in order to allow system access, personalize the system experience and conduct support.
- The system collects special category patient health data, consisting of NHS number, demographic information (name, date of birth), past medical history and current medical history.
- Demographic information such as name, NHS number and date of birth are mandatory.
- Data can be deleted by the data controller and by the data processer upon request.
- Data controller has total ownership over data.
- Data is entered by the data controller at times when they deem appropriate, there is no requirement to enter data for any set period of time.
- Data entered into the system will likely cover the geographic area within which the Data controller operates.

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)?*

- The system stores and processes OPAT treatment data in order to allow the controller to monitor and review the patients OPAT treatment journey. This data is classified as special category patient health data.
- System reports are user defined and controlled.
- Medical data is entered via medical professionals (data controller) who should gain consent from the patient in order to do this. It is the duty of the data controller to gain consent and explain who the data will be used.
- HSP do not process the data in any way except for the purposes specifically stated in the contract in order for us to comply with our responsibilities as a data processor.
- We make it clear to the data controller in the form of a signed contract that it is their responsibility to ensure they complain with all requirements set upon them within the Data Protection Act 2018.

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?*

The system processes data around the patient's treatment and stores it in an easily structured manner. This replaces the need for written documents and excel sheets which are insecure. Allowing data to be recorded, validating and accessed via the PMS prevents treatment errors and improves patient safety. Reports can be used to help justify service spend and help with improving patient treatment pathways.

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?

Security and data processing has been reviewed internally with applicable stake holders.

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?*

- We do not run any processes beyond the ability for the User (data controller) to collect and record their own data.
- Data quality and minimization is ensured by the User.
- Additional functionality is developed in conjunction with the User.
- No international data transfers will take place.
- We process data based on "Article 6(1)(b) – contract".
- We have a contractual obligation to process the data on before of the data Controller in order for them to efficiently and legally use our product.
- We meet with our requirements as a Data Processor by allowing the Controller to export and audit their down data.

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.*	**Likelihood of harm**	**Severity of harm**	**Overall risk**

Describe source of risk and nature of potential impact on individuals	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
REDACTED	REDACTED	REDACTED	REDACTED

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**	**Residual risk**	**Measure approved**

REDACTED	REDACTED	REDACTED	REDACTED	REDACTED

Step 7: Sign off and record outcomes

Item	Name/date	Notes

Measures approved by:	Dave Russell 01/10/2018	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Dave Russell 01/10/2018	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	n/a – no "high" risks	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: n/a		
DPO advice accepted or overruled by:	n/a	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	n/a no differing views.	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Luke Hudson	The DPO should also review ongoing compliance with DPIA