Standard Operating Procedure

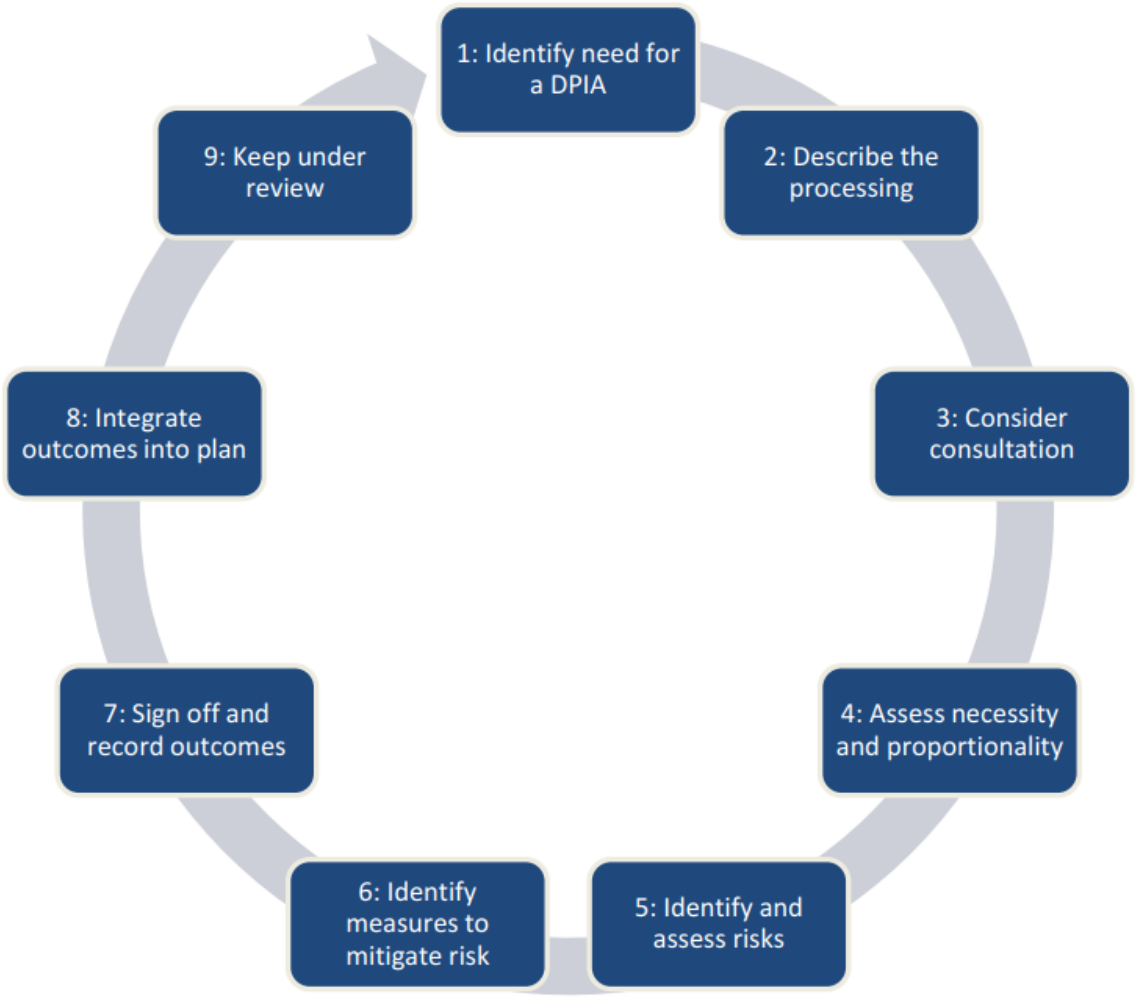
DATA PROTECTION IMPACT ASSESSENTS

SETTING Trust-wide

FOR STAFF Information asset owners, project leads and others managing new or changing personal data handling processes.

Standard Operating Procedure (SOP)

A data protection impact assessment (DPIA) should begin early in the life of a project, before you start your processing, and run alongside the planning and development process. It is an iterative process and includes these steps:



Note: This SOP requires use of the DPIA workbook which uses an Excel format. This will be a living and evolving document. Care must be taken over version control when using the workbook and copies saved at appropriate stages.

Step 1: Is a DPIA required

Note: step1 includes step 2 on the first iteration of the DPIA. References in curly brackets {} are to questions in the DPIA Workbook.

You should use the screening tab of the DPIA workbook as soon as you commence a new or change project which uses personal data. In a small number of cases, including research projects, where it is known a DPIA will be carried out or has been carried out elsewhere, this is not required. If in doubt consult the data protection officer (DPO).

The preliminary question asks you to consider whether the processing is one of the mandatory types where a DPIA is required either by General Data Protection Regulations (GDPR) or by Information Commissioner's Office (ICO) direction. The list is on a separate tab. If the answer is "Yes" a DPIA will be required. You must however still complete the additional questions as these will capture some required information which is not duplicated in the full DPIA.

On completion of the screening exercise submit the workbook to the DPO who will advise on your decision whether to proceed with a full DPIA. The DPO will keep a copy of the completed screening. As in all steps this may be iterative. The DPO may seek further information before signing off the screening. Answer any comments or queries raised by the DPO and resubmit the screening.

If the decision is that no DPIA is required that is all you need to do. If a DPIA is required make sure that Step 2 has been completed as fully as possible and proceed to Step 3.

Step 2: How do we describe the processing?

Although most relevant to a full DPIA, this must be done as fully as possible as part of the Step 1 screening and is included on the screening tab of the workbook. It is essential for documenting that proper consideration was given and to enable the DPO to assess the screening.

Describe how and why you plan to use the personal data. Your description must include "the nature, scope, context and purposes of the processing". This may be done directly in the workbook or you may prefer to refer to a separate document (such as a project initiation document) for a complex issue. It may be easier to answer the screening questions first - you will not need to repeat information from answering those questions in the general description.

The nature of the processing is what you plan to do with the personal data. This should include, for example:

- how you collect the data;
- how you store the data;
- how you use the data;
- who has access to the data;
- whether you will use any processors;
- security measures;

{Screening and DPIA Q1}.

The scope of the processing is what the processing covers. This should include, for example:

- the nature of the personal data;
- the volume and variety of the personal data;
- the sensitivity of the personal data;
- the extent and frequency of the processing;
- the duration of the processing;
- the number of data subjects involved;

{Screening and DPIA Q1}.

The context of the processing is the wider picture, including internal and external factors which might affect expectations or impact. This might include, for example:

- the source of the data;
- the nature of your relationship with the individuals;
- the extent to which individuals have control over their data;
- the extent to which individuals are likely to expect the processing;
- whether they include children or other vulnerable people;
- any previous experience of this type of processing;
- any relevant advances in technology or security;
- any current issues of public concern;

{Screening}.

The purpose of the processing {Screening} is the reason why you want to process the personal data. This should include:

- the intended outcome for individuals;
- the expected benefits for you or for society as a whole.

In short as full a description of the intended processing or change as you can manage.

Also consider whether the purposes of any partners with whom the data may be shared are compatible {DPIA Q12}.

Step 3a: Do we need to consult individuals?

{DPIA Q2} You will now be completing the main DPIA workbook. The questions can be tackled in any order but it is sensible to consider consultation requirements early on. The workbook can be submitted at any stage to the DPO for advice – even if only a few questions have been answered. A good example would be if you decide not to consult on a major project – it would be sensible to seek the DPO's views.

You should always consider whether it is appropriate to consult the individuals who will be affected (or their representatives). This can use existing patient and staff (including unions) consultation processes. Reasons not to consult may include where consultation would compromise commercial confidentiality, undermine security, or be disproportionate or impracticable.

If the DPIA covers a plan to collect the personal data of individuals you have not yet identified, you may need to carry out a more general public consultation process, or targeted research. This could take the form of carrying out market research with a certain demographic or contacting
relevant groups for their views.

If your DPIA decision is at odds with the views of individuals, you need to be particular clear in documenting your reasons for disregarding their views.

Step 3b: Do we need to consult anyone else?

Consultation with the DPO is a mandatory and integral part of this process.

{DPIA Q2} If you use a data processor, you may need to ask them for information and assistance. Your contracts with processors should require them to assist. Sometimes you may

not know who a contract may be awarded to but it should always be possible to seek views. The Trust's procurement specialists may be able to advise.
You should consult all relevant internal stakeholders, in particular in relation to information security, and the Caldicott Guardian where patients are involved. Legal Services may also need to be involved. It is likely the DPO will advise this when needed.

Step 4: How do we assess necessity and proportionality?

A full description of the processing at Step 2 will help you here. You should consider:

- Do your plans help to achieve your purpose?
- Is there any other reasonable way to achieve the same result?

The workbook is designed to ensure data protection compliance, which is a good measure of necessity and proportionality. In particular, you should include relevant details of:

- your lawful basis for the processing;
- how you will prevent function creep {DPIA Q15, Q16};
- how you intend to ensure data quality {DPIA Q13, Q18, Q19};
- how you intend to ensure data minimisation {DPIA Q9, Q14};
- how you intend to provide privacy information to individuals {DPIA Q11};
- how you implement and support individuals rights {DPIA Q10, Q17};
- measures to ensure your processors comply;
- safeguards for international transfers {DPIA 28}.

{ DPIA Q4, Q5, Q6} When considering lawful basis you need to identify a condition from Article 6 GDPR. The likely ones are:

- Consent;
- Performance of a contract with data subject;
- Compliance with a legal obligation;
- Vital interests;
- Public task/official authority.

The latter needs to be based on an identified statutory duty. If in doubt the DPO can advise.

Where special category data is involved including all health data you also need a condition from Article 9:

- Explicit consent;
- Employment/social security/social protection obligations;
- Vital interests;
- legal claims;
- substantial public interest;
- medical purposes including management of health systems;
- public health;
- research.

Step 5: How do we identify and assess risks?

Consider the potential impact on individuals and any harm or damage that might be caused by your processing – whether physical, emotional or material. In particular consider whether the processing could possibly contribute to {DPIA Q25-28}:

- inability to exercise rights (including but not limited to privacy rights) {DPIA Q23};

- inability to access services or opportunities;
- loss of control over the use of personal data including marketing {DPIA Q24};
- keeping data longer than necessary {DPIA Q20, Q21, Q22};
- discrimination {DPIA Q8};
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality {DPIA Q6, Q7};
- re-identification of pseudonymised data;
- any other significant economic or social disadvantage or interference with privacy {DPIA Q8}.

You should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach (including illegitimate access to, modification of or loss of personal data) {DPIA Q25-28}.

To assess whether the risk is a high risk, you need consider both the likelihood and severity of the possible harm. Harm does not have to be inevitable to qualify as a risk or a high risk. It must be more than remote, but any significant possibility of very serious harm may still be enough to qualify as a high risk. Equally, a high probability of widespread but more minor harm might still count as high risk.

You must make an 'objective assessment' of the risks. The Trust's standard risk assessment matrix will assist.

Do not overlook corporate risks, such as the impact of regulatory action by the ICO, reputational damage or loss of public trust.

Step 6: How do we identify mitigating measures?

Typical options for mitigating data protection risks include {DPIA Q25-28}:

- deciding not to collect certain types of data – this can be as simple as not asking for a phone number if you are not intending to use it;
- reducing the scope of the processing;
- reducing retention periods;
- taking additional technological security measures including secure disposal & deletion of information;
- training staff to ensure risks are anticipated and managed;
- anonymising or pseudonymising data where possible;
- writing internal guidance or processes to avoid risks;
- adding a human element to review automated decisions;
- using a different technology;
- putting clear data sharing agreements into place {DPIA Q12};
- making changes to privacy notices { DPIA Q3, Q11};
- offering individuals the chance to opt out where appropriate;
- implementing new systems to help individuals to exercise their rights.

Record whether the measure would reduce or eliminate the risk. You ***can*** take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

Step 7: How do we conclude our DPIA?

When you have completed the workbook you need to assess whether the overall level of 'residual risk' is high, taking into account the steps you will be taking to eliminate, reduce, or accept the identified risks. You do not always have to eliminate every risk. You may decide that some risks, and even a high risk, are acceptable given the benefits of the processing and the difficulties of mitigation.

The Assessment should then be sent again to the DPO who will consider whether the final assessment is compliant.

Once everything is finalised the DPO will ask the senior information risk officer (SIRO) to sign off the assessment.

Note: The DPO role is advisory. You may decide not to follow DPO recommendations. If you decide not to follow the advice, you need to record your reasons and ask the DPO to submit the Assessment to the SIRO in any event. You should also clearly record any reasons for going against the views of other individuals or consultees.

In the (highly unusual) case that the residual risk remains high it will be necessary to consult the ICO before any processing takes place. The DPO will arrange this once authorised by the SIRO.

You should also record any reasons for going against the views of individuals or other consultees.

Step 8: What happens next?

You must integrate the outcomes of the DPIA back into your project plans. You should identify any action points and who is responsible for implementing them. You can use the usual project management processes to ensure these are followed through.

You should monitor the ongoing performance of the DPIA. You may need to cycle through the process again (even after SIRO approval) before your plans are finalised. Make the appropriate adjustments and resubmit to the DPO from any step of the cycle.

Note that DPIAs may be published to aid transparency and accountability. This could help foster trust in your processing activities, and improve individuals' ability to exercise their rights. If not published they may be disclosable under Freedom of Information - privacy impact assessments are included in the definition documents for publication schemes. If you are concerned that publication might reveal commercially sensitive information, undermine security or cause other risks, you should consider whether you can redact (black out) or remove sensitive details, or publish a summary.

You need to keep your DPIA under review, and you may need to repeat it if there is a substantial change to the nature, scope, context or purposes of your processing. Relevant DPIAs should always be considered by information asset owners when reviewing the ongoing use of the assets for which they are responsible.

RELATED DOCUMENTS	DPIA Guidance http://nww.avon.nhs.uk/dms/download.aspx?did=21751 DPIA Workbook http://nww.avon.nhs.uk/dms/download.aspx?did=21753 Risk Management Policy http://nww.avon.nhs.uk/dms/download.aspx?did=15615 Information Commissioner Privacy Impact Code of Practice Article 29 Working Party Guidance
AUTHORISING BODY	Information Risk Management Group
QUERIES	Contact: Data Protection Officer InformationGovernance@UHBristol.nhs.uk