Annex one

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

Will the project involve the collection of new information about individuals? No. It will enable the collection of some data through online forms which is currently gathered by other means such as word-processing documents or paper records.

Will the project compel individuals to provide information about themselves? No.

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? No, although the project will make access to information easier and more immediate for staff and their managers.

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? Yes. The project will enable easier access to and more timely use of information, to help staff make better use of their time and to improve Trust performance for patients.

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. No.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? Yes. Better access to the information will help staff keep up-to-date and provide them with an organisation-wide view to assess their performance and training needs. It should also give managers further means to identify achievements, support and training requirements

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For

example, health records, criminal records or other information that people would consider to be private. No.

Will the project require you to contact individuals in ways that they may find intrusive? No.

Annex two

Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.
You may find it helpful to link to other relevant documents related to the project, for example a project proposal. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

The project aims to enable clinical staff to perform a variety of administrative tasks, using data collected in the Data Warehouse

- to maintain a portfolio of the types of cases they have attended and treatment they have given, though not including patient PII, using details already recorded in the ePCR (electronic Patient Care Recording) system, to use in planning their training and as supporting evidence for HCPC certification and in performance reviews
- to complete documents such as self-assessments, hot debrief details and the results of rideouts, using online forms
- to display details of drug treatment, impression and intervention statistics for individuals and groups (again, not including any patient PII)
- to notify staff of Patient Care Updates and to show managers who has accessed them
- to enable clinical staff and their managers to view Care bundle delivery and to compare the achievements of individuals and groups across the Trust
- to provide links to other Trust systems such as Medicines Management and Incident reporting

Although measures are taken to anonymise patient data, the individually-identifiable details of staff activity, performance, qualifications, training and requirements are viewed as PII

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Details of cases including treatments and interventions by staff will be obtained from existing systems via the Data Warehouse and used to help them collect supporting evidence of their experience in preparing for assessments and certification. Patient PII will not be included, and any reports or displays showing individually identifiable performance or training information will be visible only to the individual data subjects and the managers responsible for them.

Staff PII collected through online forms will be visible only to the data subjects and their managers

Reminder – to maintain equivalent control to access to data containing staff PII collected through the CARE project if it is copied to downstream systems such as the Data Warehouse

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Clinical team representatives as system owners, IT and Informatics IG team to be consulted before changes to system functionality or access take place

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex three can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Unauthorised access to patient PII	Confidential information being available unnecessarily	Unauthorised access to PII Breaching DPA	**Loss of patient's confidence in the Organisation** **Law suits** **ICO involvement and monitory fines**
Access to records of staff activity, performance, training and support by persons other than the data subject and their managers	Confidential information being exposed	Unauthorised access to PII Breaching DPA	Staff dissatisfaction Complaints Possible legal action ICO involvement and monitory fines

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Unauthorised access to patient PII	Avoid inclusion of patient PII in all sets of data used by the project	Eliminated	Yes

Access to records of staff activity, performance, training and support by persons other than the data subject and their managers	Restrict access to all system functions by • using standard NEAS login authentication • using NEAS standard security measures for mobile devices • limiting views of data to data subjects and their managers by use of Active Directory and ESR information	Reduced	Yes

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
Unauthorised access to patient PII	Avoid inclusion of patient PII in all sets of data used by the project	IG
Access to records of staff activity, performance, training and support by persons other than the data subject and their managers	Restrict access to all system functions by • using standard NEAS login authentication • using NEAS standard security measures for mobile devices • limiting views of data to data subjects and their managers by use of Active Directory and ESR information	IG

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for

implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Avoid inclusion of patient PII in all sets of data used by the project	May 2017	RM/MB
Restrict access to all system functions by • using standard NEAS login authentication • using NEAS standard security measures for mobile devices • limiting views of data to data subjects and their managers by use of Active Directory and ESR information	May 2017	RM/MB

Contact point for future privacy concerns
Marc Birkett

Annex three

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?