Privacy Impact Assessments (PIA) – 2019006

Privacy impact assessment screening questions

These questions are intended to help organisations 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 which fits more closely with the types of project you are likely to assess.

Will the project involve the collection of new information about individuals?

Yes

Will the project compel individuals to provide information about themselves?

Yes

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

No

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

Does the project involve you using new technology which 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 which can have a significant impact on them?

No

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 particularly private.

Yes

Will the project require you to contact individuals in ways which they may find intrusive?

No

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 which is used in this code of practice. You can adapt the process and this template to produce something which 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).

A PIA was needed because we answered “Yes” to four screening questions.

Step two: Describe the information flows

The collection, use and deletion of personal data should be described 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.

The data is collected by FormStack from users completing the online form on our website. The information is hosted in a secure portal which has two factor authentication enabled for all users and all submission data is encrypted. A notification email is sent to the practice containing all submission data which is encrypted using PGP. Data is added to the EMIS clinical record. No data processing is performed by FormStack.

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.

Consultation can be used at any stage of the PIA process.

All notification emails are protected by 4096 Bit PGP Encryption. A password and encryption key is required to open the emails. Access to the secure portal is restricted to key users and all database data is encrypted. Each secure portal user has unique login credentials and require two factor authentication. Passwords expire after 90 days.

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.

Privacy Issue	Risk to individuals	Compliance risk	Associated organisation/ corporate risk
Non-secure email communication	Personal data sent via non-secured email	GDPR Breach	

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. 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?
Personal data sent via non-secured email	Use of Secure Portal to collect data. Submission data is encrypted within Secure Portal. Notification emails are encrypted with 4096 Bit PGP Encryption. Portal requires two factor user authentication and password resets every 90 days.	Risk eliminated	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
Personal data sent via non-secured email	Use of Secure Portal to collect data. Submission data is encrypted within Secure Portal. Notification emails are encrypted with 4096 Bit PGP Encryption. Portal requires two factor user authentication and password resets every 90 days.	Gareth Hannam – IG & IT Manager

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 which may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Personal data sent via non-secured email	16th August 2019	Gareth Hannam – IG & IT Manager

Contact point for future privacy concerns
Gareth Hannam – gareth.hannam@nhs.net

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?

Yes

How will individuals be told about the use of their personal data?

FormStack will be added to the Privacy Notice for Direct Care

Do you need to amend your privacy notices?

Yes

Have you established which conditions for processing apply?

Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'.

Article 9(2)(h) 'necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services..."

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?

N/A

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?

No

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

The system will enable patients to be able to send information to us in a secure way to be involved in the management of their health care and ensure we have up to date information.

Are your actions a proportionate response to the social need?

Yes

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?

Formstack will only be used for purposes of direct care.

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

No

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 information you are using of good enough quality for the purposes it is used for?

Yes

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

None

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?

Yes

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

Data is provided by the patient

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?

All data collected by the system will be downloaded securely and added to the EMIS clinical system and retained in line with the medical records retention period.

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

Yes

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?

No

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

N/A

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?

No

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

Internal training will be provided for users on the Formstack Portal

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?

Formstack complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States, respectively. Formstack has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms of this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/.
With respect to personal data transferred pursuant to the Privacy Shield Framework, Formstack is subject to regulatory enforcement powers of the US Federal Trade Commission.

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

4096 Bit PGP Encryption