# 

# Privacy Impact Assessments

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential therefore, when considering or implementing any new initiatives, that the impact of the collection, use and disclosure of any patient information is considered in regards to the individual’s privacy. Carrying out a privacy impact assessment (PIA) is a systematic way of doing this.

A Privacy Impact Assessment (PIA) is a process that helps an organisation to identify privacy risks and ensure lawful practice when a new project is designed or changes are made to a service. The purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. It is a particularly useful tool for organisations to identify privacy risks and ensure lawful practice use when:

* Planning a new information sharing initiative such as working with new partners or in different ways;
* Introducing new IT systems for collecting and accessing personal data;
* Intending to use personal data for new uses.

## What are privacy risks?

Privacy risks include the following:

* Risks to individuals or other third parties (for example, misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency).
* Compliance risks e.g. breach of the Data Protection Act (DPA)
* Risks to the organisation (for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public).

**The patient / Service User Perspective**

It helps an organisation to see things from the patient’s point of view. It is their data that is being used and their choice about how and why it will be used. “No decision about me, without me” is the vision for the patient-centred NHS. Understanding the impact to the individual(s) personal data enables the system to be designed around their legal rights and expectations of confidentiality.

A PIA also checks organisational compliance against the legal framework.

# Where do you start?

A lead person should be nominated to co-ordinate the PIA process.

A PIA starts with a screening process. The screening questions are provided in the table on the next page. Answering the screening questions will identify whether or not the proposed initiative will impact on patient privacy and whether or not you need to complete a full PIA. The screening questions are designed to give you a quick sense of the scale of the privacy issues that you may be facing.

If you answer “yes” or “unsure” to any of the screening questions in the table, you will need to undertake the PIA. You may find it helpful to seek assistance from an information governance expert to help you with the process.

# PIA screening questions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Documenting here which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template. This will also assist in ensuring that the investment the organisation makes is proportionate to the risks involved:  Remember! – imagine this initiative involved the use of your own information or that of a relative | | | | | |
|  | | **Yes** | **No** | **Unsure** | **Comments** |
| i | Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private? |  |  |  |  |
| ii | Will the initiative involve the collection of new information about individuals? |  |  |  |  |
| iii | Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? |  |  |  |  |
| iv | Will the initiative require you to contact individuals in ways which they may find intrusive[[1]](#footnote-1)? |  |  |  |  |
| v | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? |  |  |  |  |
| vi | Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition? |  |  |  |  |
| vii | Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them? |  |  |  |  |

If you answered **No** to all of the above, and you can evidence/justify your answers in the comments box above, you do not need to continue with the Privacy Impact Assessment as it will not apply to the initiative. Should the initiative change to incorporate informational privacy at any point in the future you will need to complete the screening questions again.

**Conducting a PIA**

## What should a PIA include?

In simple terms the PIA should:-

* set out the aims or objectives of the initiative
* explain why the PIA is necessary (the initial screening questions at the beginning of the template will enable this to be quickly identified)
* document the data flows in terms of, what data is being processed, where it is coming from and who it is going to
* identify the risks to individual’s privacy in terms of security, and as potential threats to confidentiality, integrity or availability
* clarify the legal basis
* Identify and evaluate the privacy solutions (how can you reduce or remove the risk?)
* Sign off and record the PIA outcomes
* Integrate the outcomes into the project plan
* Consult with internal and external stakeholders, as needed, throughout the process

## Who should be part of the PIA team needed to complete the template?

For the PIA to be effective it needs input from people with a range of expertise, skills and authority. Important features for members of the team include:

* An understanding of the project’s aims and the organisation’s culture;
* Authority to influence the design and development of the project and participate in decisions;
* Expertise in privacy and compliance matters;
* Ability to assess and communicate organisational risks;
* Ability to assess which privacy solutions are feasible for the relevant project; and
* Ability to communicate effectively with stakeholders and management.

## Does my project need a PIA?

Whilst a PIA is not a legal requirement the ICO may often ask an organisation whether they have carried out a PIA. If your project is new, or you are planning changes to an existing system, then the time is right for conducting a PIA. A PIA is suitable for:

* A new IT system for storing and accessing personal data
* A data sharing initiative where two or more organisations seek to pool or link sets of personal data
* A proposal to identify people in a particular group or demographic and initiate a course of action
* Using existing data for a new and unexpected or more intrusive purpose
* A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system
* A new database which consolidates information held by separate parts of an organisation
* Legislation, policy or strategies which will impact on privacy through the collection of personal information, or through surveillance or other monitoring
* Long standing databases where the privacy impact may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues

**Privacy Impact Assessment Template**

**Section 1: Background Information**

|  |  |
| --- | --- |
| Project Name |  |
| Organisation |  |
| Assessment Completed By |  |
| Job Title |  |
| Date completed |  |
| Phone |  |
| E-mail |  |
| Project/Change Outline - What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required. | |
|  | |
| Purpose / Objectives - Why is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project. | |
|  | |
| What is the purpose of collecting the information within the system? For example patient treatment, patient administration, research, audit, reporting, staff administration etc. | |
|  | |
| What are the potential privacy impacts of this proposal - how will this change impact upon the data subject? Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing. | |
|  | |
| Provide details of any previous Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a PIA may have been undertaken during the project implementation | |
|  | |
| Stakeholders - who is involved in this project/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change. | |
|  | |

**Section 2: The Data Involved**

|  |  |  |  |
| --- | --- | --- | --- |
| What data is being collected, shared or used?  (If there is a chart or diagram to explain attach it as an appendix) | | | |
|  | **Data Type** | | **Justifications –** there must be justification for collecting the particular items and these must be specified here – consider which data items you could remove, without compromising the needs of the project? |
| Information that identifies the individual and their personal characteristics | Name |  |  |
| Address |  |
| Postcode |  |
| Dob |  |
| Age |  |
| Sex |  |
| Gender |  |
| Racial/ethnic origin |  |
| Tel no. |  |
| Physical description |  |
| NHS no. |  |
| Mobile/home phone no. |  |
| Email address |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | Yes | N/A | **Justification** |
| Information relating to the individual’s physical or mental health or condition |  |  |  |
| Information relating to the individual’s sexual life |  |  |  |
| Information relating to the family of the individual and the individuals lifestyle and social circumstances |  |  |  |
| Information relating to any offences committed or alleged to be committed by the individual |  |  |  |
| Information relating to criminal proceedings, outcomes and sentences regarding the individual |  |  |  |
| Information which relates to the education and any professional training of the individual |  |  |  |
| Employment and career history |  |  |  |
| Information relating to the financial affairs of the individual |  |  |  |
| Information relating to the individual’s religion or other beliefs |  |  |  |
| Information relating to the individual’s membership of a trade union |  |  |  |

**Section 3: Assessment**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Question | Response | Required Action  E.g. Seek Information Governance advice |
| Legal compliance – is it fair and lawful? | 1. What is the legal basis for processing the information? *This should include which conditions for processing under the Data Protection Act 1998 apply* *and the common law duty of confidentiality.* |  |  |
| 1. a - Is the processing of individual’s information likely to interfere with the ‘right to privacy’ under Article 8 of the Human Rights Act?   b - Have you identified the social need and aims of the initiative and are the planned actions a proportionate response to the social need? |  |  |
| 1. It is important that individuals affected by the initiative are informed as to what is happening with their information. Is this covered by fair processing information already provided to individuals or is a new or revised communication needed? |  |  |
| 1. If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn? |  |  |
| Purpose | 1. Does the project involve the use of existing personal data for new purposes? |  |  |
| 1. Are potential new purposes likely to be identified as the scope of the project expands? |  |  |
| Adequacy | 1. Is the information you are using likely to be of good enough quality for the purposes it is used for? |  |  |
| Accurate and up to date | 1. Are you able to amend information when necessary to ensure it is up to date? |  |  |
| 1. How are you ensuring that personal data obtained from individuals or other organisations is accurate? |  |  |
| Retention | 1. What are the retention periods for the personal information and how will this be implemented? |  |  |
| 1. Are there any exceptional circumstances for retaining certain data for longer than the normal period? |  |  |
| 1. How will information be fully anonymised or destroyed after it is no longer necessary? |  |  |
| Rights of the individual | 1. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held? |  |  |
| Appropriate technical and organisational measures | 1. What procedures are in place to ensure that all staff with access to the information have adequate information governance training? |  |  |
| 1. If you are using an electronic system to process the information, what security measures are in place? |  |  |
| 1. How will the information be provided, collated and used? |  |  |
| 1. What security measures will be used to transfer the identifiable information? |  |  |
| Transfers both internal and external including outside of the EEA | 1. Will individual’s personal information be disclosed internally/externally in identifiable form and if so to who, how and why? |  |  |
| 1. Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data? |  |  |
| Consultation | 1. Who should you consult to identify the privacy risks and how will you do this? Identify both internal and external stakeholders. *Link back to stakeholders on page 3.* |  |  |
| 1. Following the consultation – what privacy risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc. |  |  |
| Guidance used | 1. List any national guidance applicable to the initiative that is referred to. |  |  |

## Section 3 – Privacy issues identified and risk analysis

### Identify the privacy and related risks (see Appendix 1 for further information)

*Nb. By allocating a reference number to each identified privacy issue will ensure you link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified in column*

*Table 1*

| **Ref No.** | **Privacy issue –** element of the initiative that gives rise to the risk | 1. **Risk to individuals** *(complete if appropriate to issue or put not applicable)* | 1. **Compliance risk**   *(complete if appropriate to issue or put not applicable)* | 1. **Associated organisation/corporate risk** *(complete if appropriate to issue or put not applicable)* |
| --- | --- | --- | --- | --- |
| *PR1* | *Individuals are not aware of the initiative as no communication materials have been planned* | *Individuals not aware that their data is being processed* | *Non-compliance with DPA principle 1 – fair and lawful processing* | 1. *May lead to public mistrust* 2. *May lead to sanction by the Information Commissioners office (ICO)* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 

### Identify the privacy solutions

*Table 2*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Ref No.** | **Risk – taken from column (a), (b) and/or (c) in table 1.** | **Risk score – see tables at Appendix 2** | | | **Proposed solution(s)**  **/mitigating action(s)** | **Result:** is the risk accepted, eliminated, or reduced? | **Risk to individuals is now OK?**  **Signed off by?** |
| **Likelihood** | **Impact** | **RAG status** |  |  |  |
| *PR1* | *Individuals not aware that their data is being processed*  *Non-compliance with DPA principle 1 – fair and lawful processing*  *1. May lead to public mistrust*  *2. May lead to sanction by the Information Commissioners office (ICO)* | 5 | 5 |  | *Communication plan to be developed to ensure compliance with fair and lawful processing*  *Assurance that there will be an active communication campaign*  *All relevant staff informed of need to understand and disseminate communication material.* | *Reduced to an acceptable level (it is not possible to eliminate at this stage as the Comms plan will need to ensure it addresses all aspects to enable individuals to be fully informed.* | *Yes*  *Sign-of tbc* |
|  |  |  |  |  |  |  |  |

### Integrate the PIA outcomes back into the project plan

*NB. This must include any actions identified in Table 1 and Table 2.*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Who is responsible for integrating the PIA outcomes back in to 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?** | | | | | | | |
| **Ref No.** | **Action to be taken** | **Date for completion of actions** | **Anticipated risk score following mitigation** | | | **Responsibility for action – *job title not names*** | **Current status/progress** |
| **Likelihood** | **Impact** | **RAG status** |
| *PR1* | *Communications plan to be developed* |  | *2* | *2* |  | *Project Manager to liaise with Communication lead and embed into project plan* | *Meeting arranged with Communication Lead* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Appendix 1: Types of privacy risk

**Risks to individuals**

* Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
* The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
* New surveillance methods may be an unjustified intrusion on their privacy.
* Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
* The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
* Identifiers might be collected and linked which prevent people from using a service anonymously.
* Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
* Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
* Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
* If a retention period is not established information might be used for longer than necessary.

**Compliance risk**

* Non-compliance with the common law duty of confidentiality
* Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015
* Non-compliance with the DPA.
* Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
* Non-compliance with sector specific legislation or standards.
* Non-compliance with human rights legislation.

**Associated organisation/corporate risk**

* Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
* Problems which are only identified after the project has launched are more likely to require expensive fixes.
* The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
* Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
* Public distrust about how information is used can damage an organisation’s reputation and lead to loss of business.
* Data losses which damage individuals could lead to claims for compensation.

# Appendix 2: Guidance for completing a risk register

* What is the actual risk? Make sure the risk is clear and concise and articulated with appropriate use of language, suitable for the public domain.
* Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests
* Don’t reference blame to other organisations in the risk register (the register may be made available in the public domain)
* Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

**Likelihood**



**Impact**



Using the risk “RAG” rating system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

A

A/R

R

R

R

A

A

A/R

R

R

A/G

A

A

A/R

A/R

Very High -5

High - 4

Medium - 3

G

A/G

A/G

A

A

G

G

G

G

G

1

Rare

2

Unlikely

3

Possible

4

Likely

5

Almost Certain

**Likelihood**

Low - 2

Very Low - 1

**Impact**

1. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages [↑](#footnote-ref-1)