LINDSEY LODGE HOSPICE & HEALTHCARE

Data Protection Impact Assessment Policy

Contents

1. What is a data protection impact assessment?

Data protection impact assessments, or Privacy impact assessments (PIAs), is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective DPIA will be used throughout the development and implementation of a project, using existing project management processes. A DPIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved. The term project is meant in a broad and flexible way – it means any plan or proposal in an organisation, and does not need to meet an organisation's formal or technical definition of a project, for example set out in a project management methodology.

PIAs are often applied to new projects, because this allows greater scope for influencing how the project will be implemented. A DPIA can also be useful when an organisation is planning changes to an existing system. A DPIA can be used to review an existing system, but the organisation needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. The purpose of the DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be tested by consulting with people who will be working on, or affected by, the project. These can be risks to the individuals affected, in terms of the potential for damage or distress. There will also be corporate risks to the organisation carrying out the project, such as the financial and reputational impact of a data breach. Projects with higher risk levels and which are more intrusive are likely to have a higher impact on privacy.

2. What do we mean by privacy?

Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion:

- **Physical privacy** - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information
- **Informational privacy** – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. 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

DPIAs are concerned primarily with informational privacy, but an organisation can use DPIAs to assess what they think are the most relevant aspects of privacy.

Privacy risk is the risk of harm through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to those who the person it is about does not want to have it;
- used in ways that are unacceptable to or unexpected by the person it is about; or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information. Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance. The outcome of a PIA should be a minimisation of privacy risk.

3. When do I need to conduct a DPIA?

A DPIA is suitable for a variety of situations:

- ✓ 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 (for example adding Automatic number plate recognition capabilities to existing CCTV).
- ✓ 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 use of information, or through surveillance or other monitoring.

4. What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals, corporate risk and compliance with legislation.

- The measures in place to address risk, including security and to demonstrate that you comply.

Sign off and report

Once a DPIA has been completed and the risk evaluated and minimised, the conclusions will need to be included in a report that is ratified by the IG and IT subgroup. Completed DPIA's must be revisited during the lifecycle of the project / programme to ensure:

- Risks identified are still relevant

- Actions recommended to mitigate the risks have been implemented and mitigating actions are successful

DPIA flowchart

Step one: Identify the need for a DPIA

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

↓

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. This process can help to identify potential 'function creep' - unforeseen or unintended uses of the data (e.g data sharing)

↓

Step three: identify the privacy and related risks

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

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

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?

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented? Final report sign off needs to come from the IG&IT subgroup

Risk	Approved solution	Approved by

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

Who is responsible for integrating the DPIA 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
Contact point for future privacy concerns		

Appendix A Privacy Impact Template

DPIA flowchart

Step one: Identify the need for a DPIA

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 DPIA was identified

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. This process can help to identify potential ‘function creep’ - unforeseen or unintended uses of the data (e.g data sharing).

Linking the DPIA to data protection principles (appendix A) may be helpful in identifying any potential breaches.

Step three: identify the privacy and related risks

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

Privacy issue	**Risk to individuals**	**Compliance risk**	**Associated organisation / corporate risk**

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). The evaluation of each available or proposed solution would need to include costs and benefits.

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?**

Step five: Sign off and record the DPIA outcomes

Once the privacy impact assessment has been completed with proposed solutions that minimise risk, final agreement of the solution is required by the IG&IT subgroup. It would be agreed by the subgroup whether updates of the project are required. This may be necessary for larger projects.

Risk	Approved solution	Approved by

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

The assessment author or project manager would be responsible for carrying out the actions agreed. The completed Privacy Impact Assessment would need to be stored within the hospice hard drive. Any future privacy issues arising from the project may require a further PIA.

Action to be taken	Date for completion of actions	Responsibility for action
Contact point for future privacy concerns		

5. Consultation

IT & IG committee

6. Dissemination

Via Lindsey Lodge `L` drive Policies/guidelines of this form.

7. Equality Act

In accordance with the Equality Act (2010), Lindsey Lodge will make reasonable adjustments in the workplace so that an employee with a disability, as covered under the Act, should not be at any substantial disadvantage. Lindsey Lodge will endeavour to develop an environment within which individuals feel able to disclose any disability or concern which may have a long term ad substantial effect on their ability to carry out their normal day to day activities.

Lindsey Lodge will wherever practical make adjustments as deemed reasonable in light of an employee's specific circumstances and the Hospice's available resources paying particular attention to the Disability Discrimination requirements and the Equality Act (2010)

<table>
<tr><td colspan="5"><b>REFERENCES:</b>
Conducting privacy impact assessments - Code of Practice V1.0, Information Commissioner's Office</td></tr>
<tr><td colspan="5"><b>Lead Author of Policy: Dr Lucy Adcock, Caldicott Guardian</b>
<b>Responsible Sub-group</b>   Information Governance and Information Technology
<b>RATIFICATION DATE BY TRUSTEES:</b> February 2019
Review interval 2 year</td></tr>
<tr><td>TO BE REVIEWED</td><td>REVIEW COMPLETED</td><td>BY</td><td>APPROVED BY</td><td>CIRCULATION</td></tr>
<tr><td>February 2021</td><td>July 2021</td><td>KF/LA</td><td>IG/IT Sub-Group</td><td>L: Policies & Guidelines</td></tr>
<tr><td>July 2023</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>