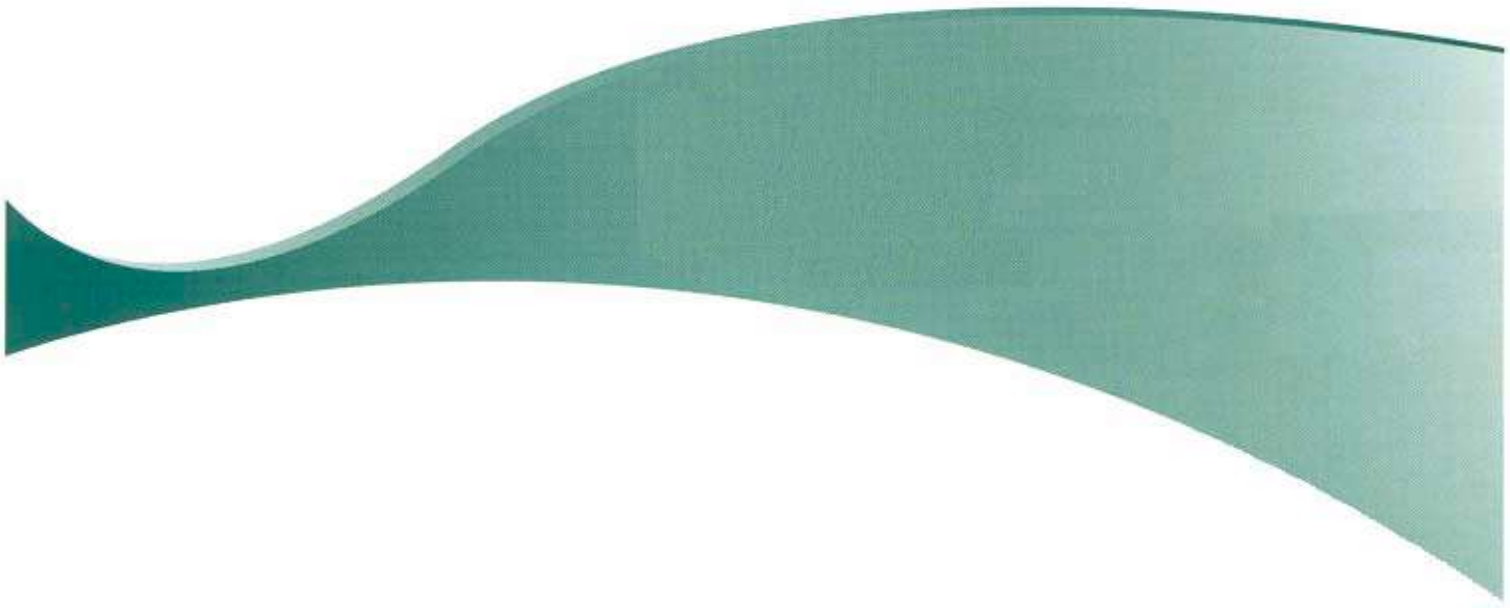
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Privacy Impact Assessment (PIA) Form

Private & Confidential



This form should be completed with reference to the HSE Privacy Impact Assessment Process Guidance Document

Version2.0

June 2019

Seirbhís Sláinte Níos Fearr á Forbairt | Building a Better Health Service

Document Information

Title:	HSE Privacy Impact Assessment (PIA) Form
Purpose:	A PIA is a process to help identify and minimise the data privacy risks of a project or activity so as to ensure that patients and service users' rights to privacy and confidentiality are appropriately protected.
Author:	Joe Ryan
Publication date:	August 2018
Review Date:	August 2020

Document History

Version	Owner	Author	Publish Date
1.0	HSE	Joe Ryan	August 2018
2.0	HSE	Joe Ryan	June 2019

Contact Details

Data Protection Officer **HSE**	Email: dpo@hse.ie Phone: 01-635 2478

Deputy Data Protection Officer West (excluding voluntary agencies) **Consumer Affairs, Merlin Park University Hospital, Galway.** • **CHO 1 – Cavan, Donegal, Leitrim, Monaghan, Sligo** • **Community Healthcare West – Galway, Mayo, Roscommon** • **Mid-West Community Healthcare – Clare, Limerick, North Tipperary.** • **Saolta Hospital Group**	Email: ddpo.west@hse.ie Phone: 091-775 373
Deputy Data Protection Officer Dublin North-East (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE DNE, Bective St., Kells, Co. Meath.** • **Midlands, Louth, Meath Community Health Organisation** • **Community Health Organisation Dublin North City & County** • **CHO 6 – Dublin South East, Dublin South & Wicklow** • **RCSI Hospital Group** • **National Children's Hospital**	Email: ddpo.dne@hse.ie Phone: Kells: 046-925 1265 Cavan: 049-437 7343
Deputy Data Protection Officer Dublin mid-Leinster (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE, Third Floor Scott Building, Midland Regional Hospital Campus, Arden Road, Tullamore, Co. Offaly.** • **Dublin Midlands Hospital Group** • **Ireland East Hospital Group** • **Community Healthcare Dublin South, Kildare & West Wicklow**	Email: ddpo.dml@hse.ie Phone: Tullamore: 057-935 7876 Naas: 045-920 105
Deputy Data Protection Officer South (excluding voluntary hospitals and agencies) **Consumer Affairs, HSE South, Ground Floor East, Model Business Park, Model Farm Road, Cork. Eircode: T12 HT02** • **Cork & Kerry Community Healthcare** • **CHO 5 – Carlow, Kilkenny, South Tipperary, Waterford & Wexford** • **UL Hospital Group** • **South South-West Hospital Group**	Email: ddpo.south@hse.ie Phone: Cork Office: 021 – 4928538 Kilkenny Office: 056 -7785598.

Privacy Impact Assessment Form

Section 1 – Initial Details (Threshold Assessment)

Title of the activity: _____

Name of person completing this form: _____

Title: _____

Service Area: _____

Is personal data being collected or used? Yes ☐ No ☐

Are special categories of personal data being collected or used? (as listed below) Yes ☐ No ☐

If yes, indicate the categories involved:

- ☐ Health data
- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Genetic data
- ☐ Biometric data

If you answered 'No' to both of the questions above you do not need to complete the remainder of the form as a PIA is not required

If you answered 'Yes' to any of the questions above you may need to complete a PIA - answer the questions below to establish if a PIA is required:

Does the processing include the processing on a large scale of special category data?

Yes ☐ No ☐

Could the processing likely result in a high risk to the rights and freedoms of data subjects?

Yes ☐ No ☐

Does the processing include a systematic monitoring of a publicly accessible area on a large scale e.g. CCTV?

Yes ☐ No ☐

Does the processing involve the automated processing, including profiling, on which decisions are based that produce legal effects concerning the data subjects?

Yes ☐ No ☐

If you have answered 'Yes' to any of the four questions above then you need to complete the remainder of this form as a PIA is required.

In order to complete this form please note that it is obligatory for you to have completed the HSELanD GDPR/Data Protection Awareness training. Please confirm that you have completed this training: Yes ☐ No ☐

Section 2 – Activity Details

Briefly outline the activity (name, purposes, context of use, etc.)

Describe how the activity generally works (from data collection to data destruction, different processing stages, storage etc.) give a detailed description of each of the processes carried out.

What is the legal basis for processing the data?

- ☐ Consent from the data subject.
- ☐ Processing is necessary for the performance of a contract.
- ☐ Processing is necessary for a legal obligation to which the HSE subject.
- ☐ Processing is necessary to protect the vital interests of the data subject.
- ☐ Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the HSE.

If processing special categories of data what is the legal basis?

- ☐ Explicit Consent
- ☐ For the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of medical care, treatment or social care, for the management of health or social care systems and services. Or pursuant to a contract with a health practitioner.
- ☐ Other (please state)

If applicable describe the relevant legal obligation (act, regulation, article etc.):

_____

Name the Data Controller(s) involved in this activity:

Describe the Role of the data controller(s) for this activity:

Provide details of all data processors involved in this activity:

Describe the role of data processor(s) as relevant to this activity:

For each data processor, describe their responsibilities (duration, scope, purpose, documented processing instructions, prior authorisation, contracts in place) for this activity:

Provide details of all data sub-processors involved in this activity:

Does the activity use automated decision making? Yes ☐ No ☐

If 'Yes' briefly describe the automated decision making

_____

_____

If 'Yes' what are the consequences of the automated decision making for the data subject:

Explain why all personal data collected is necessary for the purposes of your processing:

List the data supporting assets (hardware, software, networks, people, paper or paper transmission channels):

Is the personal data going to be shared? Yes ☐ No ☐

If yes, list the recipients (or categories of recipients) of the personal data and for what purpose it is being shared:

Is the data being sourced from another source? Yes ☐ No ☐

If yes, please state where the data originates from and if applicable, did it come from a publicly accessible source:

What is the retention period for the different items of personal data:

Describe the steps taken to ensure that the personal data is kept up to date and accurate:

How are data subjects informed of the processing?

How can data subjects exercise their right to access and to data portability under Article 15 and Article 20 of the GDPR?

How can data subjects exercise their right to rectification and erasure under Articles 16 & 17 of the GDPR?

How can data subjects exercise their right to restriction and object under Article 18 and Article 21 of the GDPR?

Is the personal data being transferred outside of the Republic of Ireland? Yes ☐ No ☐

If yes, list the countries where the personal data is to be transferred:

For each country outside of the EEA (European Economic Area) where data is stored or processed, name it and describe the provisions concerning the transfer:

Describe the organisational security measures associated with this activity:

Describe the technical security measures associated with this activity:

Describe the additional measures taken to ensure data security for this activity:

Section 3 – Research

Please complete the following section only if you are completing this PIA as part of a research proposal.

If you are not completing this PIA as part of a research proposal you can go immediately to Section 4.

Please specify what arrangements are in place to ensure that personal data will be processed as is necessary;

(a) to achieve the objective of the health research and;

(b) to ensure that data shall not be processed in such a way as to damage or distress the data subject:

The provision of training in data protection law and practice to anyone involved in carrying out the health research is a mandatory legal requirement. Please specify the data protection training undertaken by those involved in this research:

Please specify the controls in place to log whether and by whom personal data has been consulted, altered, disclosed or erased:

Please specify the arrangements to anonymise, archive or destroy personal data once the health research has been completed and how this will be carried out:

Please specify other technical and organisational measures designed to ensure that processing is carried out in accordance with the Data Protection Regulation, together with process for testing and evaluating the effectiveness of such measures:

Section 4 – Risks and Risk Mitigation	
Is there a risk of:	a. ☐ Illegitimate access to personal data b. ☐ Unwanted modification to personal data c. ☐ Personal data disappearance d. ☐ Other (please state)

Section 4 (a) – Illegitimate access to personal data

Complete the following questions if you selected a. (Illegitimate access to personal data)

What are the main threats that could lead to the risk?

What are the potential impacts on data subjects arising from the risk?

What are the risk sources?

What controls are in place to address the risk and are these controls adequate?

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	☐ 1 – Rare ☐ 2 – Unlikely ☐ 3 – Possible ☐ 4 – Likely ☐ 5 – Highly Certain
How do you estimate the potential impact of the risk on data subjects?	☐ 1 – Negligible ☐ 2 – Minor ☐ 3 – Moderate ☐ 4 – Major ☐ 5 – Critical
What is the overall risk rating (likelihood x impact)?	☐ Low ☐ Medium ☐ High

Section 4 (b) – Unwanted modification to personal data

Complete the following questions if you selected b. (Unwanted modification to personal data)

What are the main threats that could lead to the risk?

What are the potential impacts on data subjects arising from the risk?

What are the risk sources?

What controls are in place to address the risk and are these controls adequate?

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

- ☐ 1 – Rare
- ☐ 2 – Unlikely
- ☐ 3 – Possible
- ☐ 4 – Likely
- ☐ 5 – Highly Certain

How do you estimate the potential impact of the risk on data subjects?

- ☐ 1 – Negligible
- ☐ 2 – Minor
- ☐ 3 – Moderate
- ☐ 4 – Major
- ☐ 5 – Critical

What is the overall risk rating (likelihood x impact)?

- ☐ Low
- ☐ Moderate
- ☐ High

Section 4 (c) – Personal data disappearance

Complete the following questions if you selected c. (Personal data disappearance)

What are the main threats that could lead to the risk?

What are the potential impacts on data subjects arising from the risk?

What are the risk sources?

What controls are in place to address the risk and are these controls adequate?

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

- ☐ 1 – Rare
- ☐ 2 – Unlikely
- ☐ 3 – Possible
- ☐ 4 – Likely
- ☐ 5 – Highly Certain

How do you estimate the potential impact of the risk on data subjects?

- ☐ 1 – Negligible
- ☐ 2 – Minor
- ☐ 3 – Moderate
- ☐ 4 – Major
- ☐ 5 – Critical

What is the overall risk rating (likelihood x impact)?

- ☐ Low
- ☐ Moderate
- ☐ High

Section 4 (d) – Other

Complete the following questions if you selected d. (Other)

Describe in detail the risk

What are the main threats that could lead to the risk?

What are the potential impacts on data subjects arising from the risk?

What are the risk sources?

What controls are in place to address the risk and are these controls adequate?

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	☐ 1 – Rare ☐ 2 – Unlikely ☐ 3 – Possible ☐ 4 – Likely ☐ 5 – Highly Certain
How do you estimate the potential impact of the risk on data subjects?	☐ 1 – Negligible ☐ 2 – Minor ☐ 3 – Moderate ☐ 4 – Major ☐ 5 – Critical
What is the overall risk rating (likelihood x impact)?	☐ Low ☐ Medium ☐ High

Section 5 – Data Subject Consultation

Were data subjects (or a representative) consulted as a part of the PIA process? ☐ Yes ☐ No

If Yes, state the number of data subjects consulted, method of consultation and describe the outcome of the consultation:

If No, explain the reasons for not consulting data subjects:

Section 6 – DPO/DDPO Consultation
DPO opinion (please ensure the previous questions are completed fully before the DPO can provide an opinion):

Section 7 – Approval ***To be completed by the data controller***	
Outcome:	☐ Approved ☐ Denied ☐ DPC Consultation Needed ☐ Further Updates Needed
Signed: _____	**Date:** _____