NORTHERN IRELAND PRACTICE AND EDUCATION COUNCIL FOR NURSING AND MIDWIFERY

Data Protection Impact Assessment (DPIA) Policy and Procedure

November 2024

Any request for the document in another format or language will be considered

James House
2-4 Cromac Avenue
BELFAST
BT7 2JA

Tel: 0300 300 0066

https://nipec.hscni.net

Developed by:	Business Manager
Approved by / date:	**BTM:** 12th January 2021; 12th November 2024; **Council:** 4th December 2024
Date of next Review:	November 2028
Equality Screened by date:	November 2024

CONTENTS

		Page
1.	Introduction	3
2.	What is a Data Protection Impact Assessment?	3
3.	Benefits	4
4.	When is a Data Protection Impact Assessment required?	4
5.	How to undertake a Data Protection Impact Assessment	5
6.	Screening Exercise (to decide if a full DPIA is needed)	7
7.	Full Data Protection Impact Assessment	7
8.	Responsibilities	8
9.	Non-Compliance	8
10.	Equality Statement	8
11.	Review	8
Appendix 1 – HSC DPIA Template		9
Appendix 1 – Data Protection Principles		28
Appendix 2 – Lawful Basis for processing Personal Information and Special Category Information		29
Appendix 3 – Examples of possible risks include		32

1. Introduction

NIPEC must ensure that any processing of personal information for which it is responsible complies with the UK General Data Protection Regulations (UK GDPR) and the Data Protection Act (DPA) 2018.

GDPR introduced new obligations which require public authorities to integrate data protection concerns into every aspect of their processing activities. This approach, 'data protection by design' (the consideration of data protection at the very onset of any project), and 'data protection by default' (only processing the data that is necessary to achieve a specific purpose), requires NIPEC to consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle.

Under Article 35 of the UK General Data Protection Regulation (GDPR), data controllers will be legally required to undertake Data Protection Impact Assessment (DPIA) prior to data processing which is *"likely to result in a high risk to the rights and freedoms of natural persons*".

This policy will provide officers with guidance on how to assess whether a DPIA is required, and subsequently how to undertake and document a DPIA.

Specifically, this document is designed to assist in the identification and assessment of risks to personal information, as well as to assist in the documentation of envisaged safeguards and control measures in proportion to the risks identified.

2. What is a Data Protection Impact Assessment?

A DPIA is a process or tool to help an individual and/or organisation systematically analyse, identify and minimise data protection risks when processing personal information in any project – essentially, it is a tool used:

- To identify whether a proposed project is likely to impact on the privacy of individuals affected, either positively or negatively;
- To check whether your project is likely to comply with the data protection principles;
- To make decisions about whether and how to adjust the proposal to manage any privacy risks and to maximise the benefits of protecting privacy;
- As a reference point for future action as the project or process changes.

A DPIA will assess the impact of data processing operations on the protection of personal information, ensure that the protection of personal data collected as part of projects and processes is considered at the appropriate times and stages, and assess the likelihood and severity of risks for the rights and freedoms of individuals resulting from this operation. A DPIA is not required in all circumstances but is relevant for new projects or proposals and when planning to make changes to an existing system.

The term 'project' is used in this policy in its widest possible sense to refer to any activity or function where the collection or processing of personal data is being considered. It could refer to the development of a new system, database, programme or application, a new policy or initiative, an enhancement to or review of an existing process or a new way of working.

This policy will provide officers with guidance on how to assess whether a DPIA is required, and subsequently how to undertake and document a DPIA.

Specifically, this policy is designed to assist in the identification and assessment of risks to personal information, as well as to assist in the documentation of envisaged safeguards and control measures in proportion to the risks identified. As such, this policy shall also be considered integral to NIPEC's wider risk management process.

3. Benefits

A DPIA will assist NIPEC in a structured way to identify, categorise and mitigate privacy risks when processing personal information. Designing projects, or developing policies, with privacy in mind at the outset can lead to benefits which include:

- Identifying potential problems at an early stage, when addressing them will often be simpler and less costly;
- Increased staff awareness of privacy and data protection;
- Meeting our legal obligations and reducing the likelihood of a breach of data protection legislation;
- Ensuring our actions are less privacy intrusive and unlikely to have a negative impact on data subjects;
- Providing reassurance to individuals that NIPEC has followed best practice when using their personal data;
- Improved transparency, making it easier for individuals to understand how and why we are using their information;
- Building trust with people who use our services;

- Better information management practices.

4. When is a Data Protection Impact Assessment required?

Consideration of a DPIA is a mandatory requirement for any project, large or small, that:

- Involves collection of personal information – that is, information about living people, who can be identified;
- Involves information that may be used to identify, profile or target individuals;
- May result in surveillance of individuals or intrusions into their personal space or bodily privacy; or
- May otherwise affect whether people's reasonable expectations of privacy are met.

A DPIA must be carried out where a type of processing is likely to result in a high risk to the rights and freedoms of individuals (taking into account of both the likelihood and severity of any potential harm). If in doubt, a DPIA should be carried out.

With existing systems or processes the following criteria should also be considered:

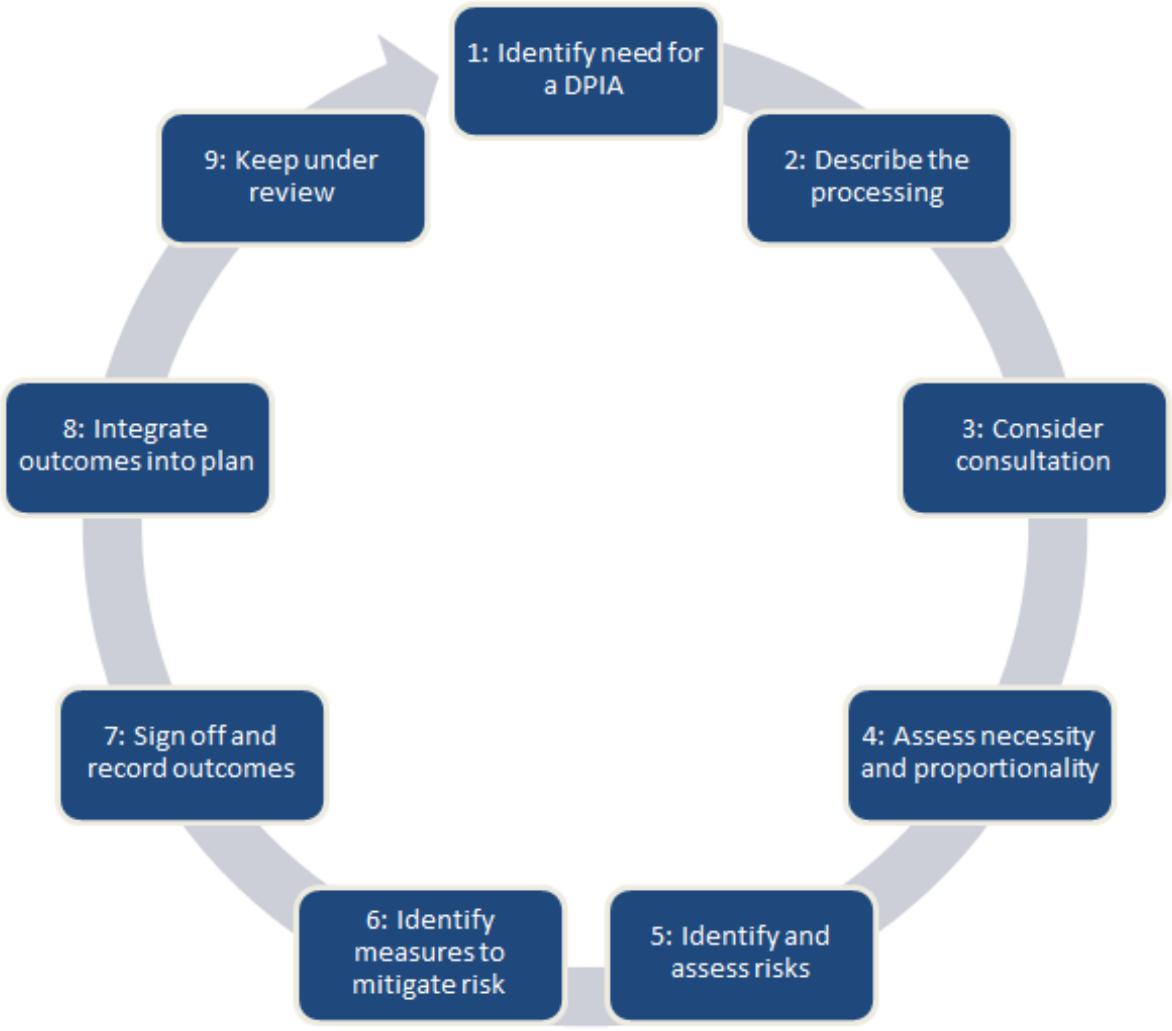
- significant changes that expand beyond the original purpose(s);
- new types of information to be processed are introduced;
- unexpected personal data breach with significant impact, the occurrence of which had not been previously identified;
- a periodic or defined review is triggered;
- in response to significant internal or external stakeholder feedback or inquiry;
- if there are technological-related changes that may have data protection implications.

5. How to undertake a Data Protection Impact Assessment

Consideration of the need for a DPIA should begin early in the life of a project before you begin processing, and run alongside the planning and development process. It includes the following steps:

- Step 1: identify the need for a DPIA
- Step 2: describe the processing

- Step 3: consultation process
- Step 4: assess necessity and proportionality
- Step 5: identify and assess risks
- Step 6: identify measures to reduce risks
- Step 7: approval process
- Step 8: implementation (integrate outcomes into project plan)



(taken from GDPR Data Protection Impact Assessments (DPIAs) ICO, March 2018)

Depending on the nature and scale of the project, a number of people should be involved in considering and undertaking a DPIA. These should include (but not be limited to) the project lead/senior manager/Information Asset Owner (IAO), project team/steering group, website governance team etc.

6. Screening Exercise (to decide if a full DPIA is needed)

At the start of any project involving the processing of personal data, the project lead/IAO will be responsible for considering the requirement for a DPIA. This involves an initial analysis of the project in question at a 'high level' and helps to decide whether or not it will be necessary to conduct a full DPIA.

The project lead/IAO may decide that the project does not require a DPIA because, for example, the project does not involve personal data, or the information used will be uncontroversial or the privacy risk is negligible. This should be formally recorded as the outcome of Step 1 and the details retained as part of the project records and will provide transparency regarding the processes undertaken. If issues around privacy considerations arise at a later stage, information within the screening exercise can be used to demonstrate accountability.

If it is decided a full DPIA is required, the Project Lead should use the regional HSC DPIA template (see Appendix 1) which allows for the recording of information in a standardised format and follows a step by step process.

7. Full Data Protection Impact Assessment (DPIA)

Following the step by step process outlined in section 5, and using information gathered from the screening exercise, the project lead/IAO should record their decisions within the full DPIA template (Appendix 1).

The completed template is the formal record of the DPIA process and should clearly document all the steps of the DPIA, contain or reference other relevant information, e.g. consultation records, and should be held alongside any business case or other project documentation, such as the PID.

Keeping a formal record will assure the public, NIPEC's Council and senior team, the ICO and other stakeholders that the project has been thoroughly assessed for risks. Once the report has been signed off, the project lead/IAO must ensure that the details of the assessment are entered in NIPEC's Information Asset Register (IAR) overseen by NIPEC's Head of Corporate Services (HoCS). The IAR is an inventory of information assets and their systems, including personal data held.

If, as a result of the new process being implemented, there will be a requirement to share personal data with another public body or organisation, the project lead/IAO, in discussion with the HoCS, must ensure that suitable arrangements are in place in the form of a robust contract or data access agreement.

8. Responsibilities

- **NIPEC Council** has overall responsibility for risk management and this includes management of information and ensuring compliance in all areas of information governance;
- The **Chief Executive** is accountable to Council for the delivery of this policy;
- The **Data Protection Officer** (DPO) will advise on the production of screening and full DPIAs;
- **All NIPEC Staff,** whether permanent, temporary, bank or agency workers, have a responsibility to ensure that they are aware of the requirements to protect personal information held by NIPEC. They are expected to familiarise themselves and adhere to this policy and relevant legislation, report any incidents in connection with this policy and take required mitigating action to ensure that incidents do not recur.

9. Non-Compliance

Compliance with this policy and any associated procedures will be monitored regularly and reports considered by the appropriate management. A failure to adhere to this policy and any associated procedures may result in disciplinary action.

10. Equality Statement

This policy has been screened for equality implications as required by Section 75 and Schedule 9 of the Northern Ireland Act 1998.

No significant equality implications have been identified therefore the policy will not be subject to an equality impact assessment.

11. Review

This policy is based on a regional HSC approach and will be monitored and reviewed in November 2028, or sooner, if a revised HSC policy is issued.

Appendix 1

Health and Social Care

HSC Data Protection Impact Assessment (DPIA) Template

What is a DPIA?

A DPIA is an assessment of the personal data used for a new, or a change to, a system or service. The assessment involves completing a document called a DPIA template. Through this process, risks and measures to mitigate those risks will be assessed. The DPIA is therefore an important document in demonstrating due diligence in terms of data privacy and security; however, it is not the formal agreement to share information or to proceed with a project or system.

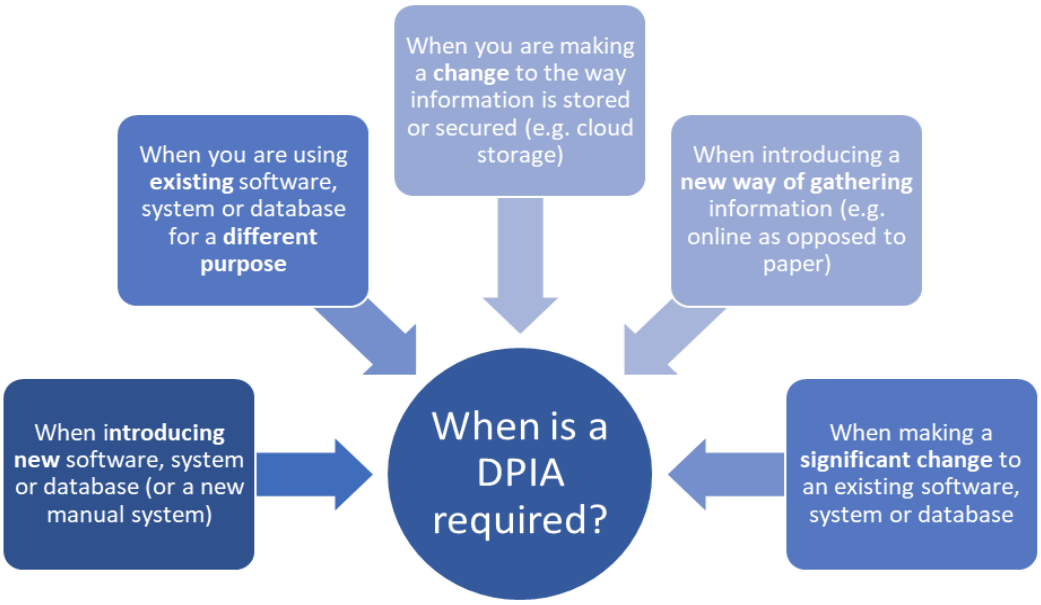
A DPIA forms part of the 'privacy by design' approach to the handling of personal information and allows services to demonstrate compliance with data protection legislation.

WHY DO A DPIA?

It is mandatory for services to complete a DPIA when introducing any new or a change to a system or service that will involve the processing of personal data.

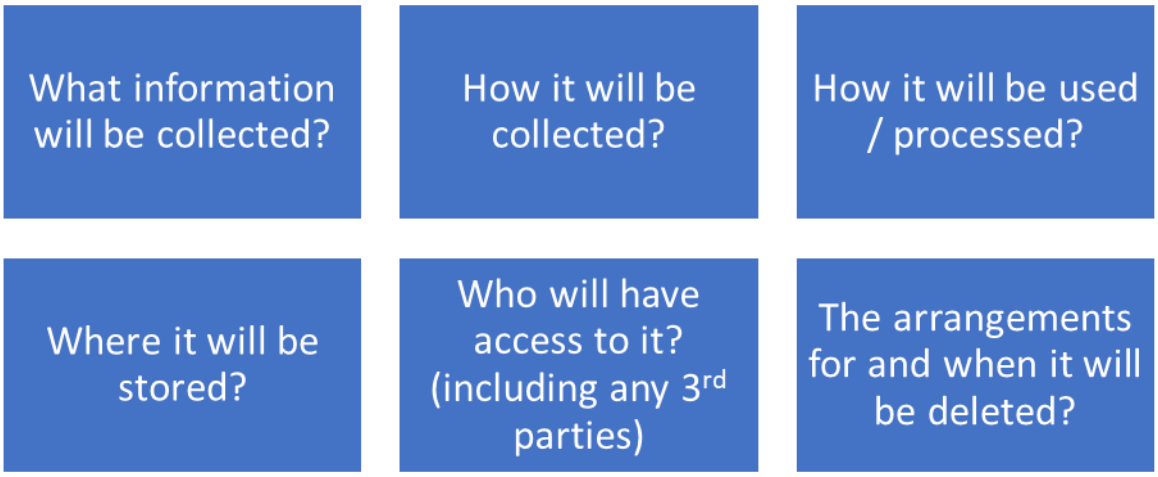
When is a DPIA required?

Data Protection applies to any process involving personal data about living individuals.



The purpose of a DPIA

Completing a DPIA will allow you to identify any privacy risks with your new system and help you to put the necessary safeguards in place to mitigate those risks. An assessment of privacy risks is only possible if you fully understand how personal data will be used. Charting the information or developing a **data flow map** is therefore a key part of the DPIA process so you must clearly describe or explain:



The data protection or privacy risks associated with a project will be closely linked to the data protection principles as set out in UK GDPR (see Appendix 3 for examples of risks).

When should you complete a DPIA?

It is important to begin completion of the DPIA at the outset of the process to avoid delays at a later stage.

Who is responsible for completing a DPIA?

Responsibility for completion of DPIAs lies with the Service Lead or Project Lead that is introducing the new system/process, responsible for that service/business area. The Service Lead or Project Lead will complete the DPIA based on their knowledge of data flows, information systems and related risks. The Information Asset Owner/IAO (a senior Manager or the Assistant Director responsible for the service area) is responsible for ensuring a DPIA is completed by the Service Lead, should be kept appraised and will provide final sign-off. The IAO will ensure that no data processing will take place until this

DPIA has been completed and signed. The IAO will also ensure that this DPIA is reviewed and updated if the data processing changes.

Who should be consulted?

Consultation is an important part of the DPIA process and should be built into all stages of the process. This may involve seeking the view from internal or external sources who can provide advice based on their area of interest or expertise (e.g. IT/ICT/Digital Services Department, Information Governance (IG) staff or external providers); or those who will be affected by the new project (e.g. staff or service users). IT/ICT/Digital Services Department approval is a separate process which sits alongside the DPIA. A DPIA focuses mainly on the data protection issues of a project or initiative. The DPIA should focus on the risks to the privacy of the data subjects.

What other documentation might be required?

The main purpose of a DPIA is to assess the data protection aspects of a new system or service. It will document the identified risks and measures that will be taken to mitigate those risks.

A DPIA is considered a "live" document and should be updated when changes to the processing occur. Conducting a DPIA is part of a wider process, e.g. procurement and as such separate documentation may also be required to support the DPIA and give context to the scope of the personal data processing, such as a Business Case, a Data Sharing Agreement or a Contract (which can be referred to within your DPIA).

What is the sign-off process for a completed DPIA?

The sign-off process for all DPIAs is:

1. Draft DPIA is completed and shared with IG Dept (and IT/ICT/Digital Services Department if applicable). Once agreed by all parties the draft version is signed off by the Project or Service Lead;

2. IG will then send it to the Data Protection Officer (DPO) to consider data protection compliance issues and advise on whether the data protection risks are identified and mitigated appropriately DPO will sign off once reviewed.

3. The DPIA is returned to Service/Project Lead to Share with their Information Asset Owner (IAO) for their consideration and approval. The IAO is required to sign off on any residual risks that cannot be mitigated. Once signed off by the project lead, DPO and IAO a copy should be returned to the IG department for logging.

Data Protection Impact Assessment (DPIA) template

The DPIA outlines

- what personal data will be processed?
- what will the information be used for?
- any risks associated with the processing.
- steps taken to mitigate against the risks.

Project/System name:
Service or Project Lead – completing the DPIA **Name:** **Telephone:** **Email Address:**
Department/Location (include full address)
Directorate:
Date DPIA commenced:
Version number:

STEP 1. DESCRIBE THE PROCESS

Briefly describe below the purpose of the data processing and what the project aims and objectives are?

Please **do not** embed documents or hyperlinks. Instead, attach relevant documents as appendices and clearly indicate which section of the appendices provides the necessary info in relation to each question below.

- **what information will be collected,**
- **how it will be collected,**
- **how it will be used / processed**
- **where it will be stored**
- **who will have access to it (including any 3rd parties)**
- **the arrangements for and when it will be deleted**

As part of this first stage, the service area may need to complete a Data Flow Map. This can be a diagram but should accurately describe the stages of the data flow from beginning to end.

If your processing includes the use of emerging technologies e.g. **Artificial Intelligence (AI)** then this needs to be specified in more detail below:

Please see the ICO's guidance on AI AI and data protection risk toolkit | ICO

STEP 2. ASSESS THE NEED FOR A DPIA				
Screening Questions- The following are intended to help decide whether a full DPIA is necessary.				
Number	Question	YES	NO	**Either way please provide further details here**
1.	Does the project involve collecting **new/additional personal information** about individuals?	☐	☐	
2.	Does the project involve gathering information in a new way?	☐	☐	
3.	Does the project establish a new way of identifying individuals?	☐	☐	
4.	Will the project use an individual's personal data already held in an existing system (manual or electronic) for a new purpose or in a new way?	☐	☐	
5.	Will the project disclose or share personal information with organisations or people/staff who have not previously had routine access to it.	☐	☐	
6.	Will the project involve matching or linking with personal information held by a different organisation(s) or departments or in different datasets e.g. combining, comparing or matching personal data obtained from multiple sources	☐	☐	

STEP 2. ASSESS THE NEED FOR A DPIA				
Screening Questions- The following are intended to help decide whether a full DPIA is necessary.				
Number	Question	YES	NO	**Either way please provide further details here**
7.	Will the project change the way personal information is managed, stored or secured (e.g. new database, new location, cloud storage)	☐	☐	
8.	Is this a system or process that has not had a DPIA completed previously? Or is there a DPIA in place but this is a new instance of processing?	New ☐ Update ☐ *If this is an update to an existing DPIA please provide details*		

If you have answered <u>YES</u> to any of the above, <u>continue to Step 3</u> and complete the DPIA.

If you have answered <u>NO</u> to all of the 8 questions above <u>please proceed to Step 12 and record the outcome</u>.

STEP 3. DESCRIBE THE PERSONAL DATA BEING COLLECTED		
What Personal data is being collected? This applies to any stage of the process (tick only those that apply). * *this list is not exhaustive*		
Personal Data required	**Tick all that apply**	**Provide details of who the personal data relates to:** i.e. Service User/staff/relative/Other (please detail)
Name	☐	
Address	☐	
Full post code	☐	
Date of Birth	☐	
Work email address	☐	
Personal email	☐	
Telephone/mobile number	☐	
National Insurance number	☐	
Health and Care number	☐	
Hospital No./System ID	☐	
Personal Images	☐	
Other* please specify all other personal data	☐	
Please provide justification for the personal data being processed e.g. Do you need full postcode or would partial postcode be sufficient? Do you need full Date of Birth or would age be sufficient?		

Special Category data (sensitive personal data)	**Tick all that apply**	**Provide details of who the Special Category data relates to:** i.e. Service User/staff/relative/Other (please detail)
Health and Social Care Data	☐	
Racial or Ethnic Origin	☐	
Biometric data (e.g.finger print, eye, face)	☐	
Genetic data	☐	
Data concerning a person's sex life/sexual orientation	☐	
Religious beliefs	☐	
Other: Political opinions ☐ Philosophical Beliefs ☐ Trade Union Membership ☐ Criminal convictions ☐		
Other data collection methods: If your processing includes monitoring/surveillance, body worn cameras, Virtual Number Plate Recognition (VNPR), CCTV, GPS, Fitness trackers, recording phone calls/voice information please provide more detail below:		

STEP 4. LAWFUL BASIS FOR PROCESSING		
What is your UK GDPR Lawful Basis for processing/sharing personal data? See Appendix 2 for further information or seek IG advice.		
Article	**Lawful basis**	**Tick**
6 1 (a)	Consent	☐
6 1 (b)	Contract	☐
6 1 (c)	Legal obligation (Please detail which legislation* this will come under)	☐
6 1 (d)	Vital Interests	☐
6 1 (e)	Public Task (please detail sections of the legislation which support Public task legal basis below)	☐
6 1 (f)	Legitimate Interests	☐
*__Relevant to 6, 1 (c) only:__ Please provide details of the relevant sections of legislation in addition to UKGDPR, which support your legal basis **Note:**		
If applicable what is your UK GDPR Lawful Basis for processing/sharing **special category data**? See Appendix 2 for further information or seek IG advice.		
Article	**Lawful Basis**	**Tick**
9 2 (a)	Consent	☐
9 2 (b)	Employment social security social protection law	☐
9 2 (c)	Vital Interests	☐
9 2 (d)	Legitimate interest	☐
9 2 (e)	Already public	☐
9 2 (f)	Establishment, exercise or defence of Legal claims or judicial capacity	☐
9 2 (g)	Public Interest	☐
9 2 (h)	Health and Social Care treatment or management of HSC systems	☐
9 2 (i)	Public Interest in the area of Public Health, Quality and Safety of Health Care	☐
9 2 (j)	Archiving in the public interest, scientific, historical research or statistical purpose	☐

STEP 5: ASSESS SECURITY OF THE INFORMATION		
Will the information be shared with, hosted by or transferred to another organisation or third party?		
If NO – move to Step 6 **If YES -** please list all the organisations who will receive or have access to the personal data being processed:		
Where will the information be:	**Sent to**	**Stored**
Within the Northern Ireland HSC	☐	☐
Outside the HSC but within the UK	☐	☐
Outside the UK but within the EU	☐	☐
Outside the EU (if outside the EU you should add this as a risk in Step 6 and detail here how will you safeguard any international transfers)	☐	☐
How will you secure the information in Transit? Tick which apply		
Encrypted Email	☐	
Shared internally over secure network	☐	
Secure file transfer	☐	
Secure Cloud Server	☐	
Amazon AWS or Microsoft Azure	☐	
Registered post via post safe envelopes / secure post service	☐	

STEP 6: ICT Input			
Have you sought approval from your IT/ICT/Digital Services Department? **If you have answered NO or N/A, state your reason and proceed to step 6**. If **YES** continue to answer the remaining questions in this section	YES ☐	NO ☐	N/A ☐

Has a 3rd party technical questionnaire/Cyber Security questionnaire been completed and approved by IT/ICT/Digital Services Department?	YES ☐	NO ☐	N/A ☐
If the cloud storage platform is not Amazon AWS or Microsoft Azure, please answer the following questions: Has the solution been PEN tested? (Penetration Tested – Please provide a copy) Does the solution have Anti-Virus software? Does the solution have Anti-Ransomware? Is multi factor authentication available?	YES ☐ YES ☐ YES ☐ YES ☐ YES ☐	NO ☐ NO ☐ NO ☐ NO ☐ NO ☐	N/A ☐

STEP 7. CONSULTATION PROCESS
You should consider the impact of the new process or system will have on all your stakeholders. Who have you consulted with? Service Users☐ IG Department ☐ IT Department☐ Legal☐ Internal/external Partners (please list) Statutory agencies (please list) ☐ Other (please list) ☐

STEP 8. EVALUATE THE PROCESS		
Function creep is the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended as set out this DPIA, especially when this leads to potential invasion of privacy. Are you content with the measure in place that there is no risk of function creep? If **No**, please ensure the risk of function creep is included at **Step 11**	YES ☐	NO ☐
What measures will be in place to ensure the accuracy and quality of the data being processed?		
What measures will be in place to ensure the data minimisation principle is adhered to? *i.e. only processing or sharing what is necessary and the minimum amount needed for the purpose.*		

STEP 9. CONSIDERATION OF DATA SUBJECTS RIGHTS		
1. Right to be informed		
Is the project covered by an existing privacy notice? (If no, a bespoke privacy notice will be required and approval sought through IG Department)	YES ☐	NO ☐
2. Right of access		
The organisation is obliged to provide personal information upon request in line with Data Protection Act 2018 and UK GDPR. Have you considered how this will be achieved in your project? Please provide details below:	YES ☐	NO ☐

STEP 10. PERSONAL INFORMATION SHARING AGREEMENTS		
Is there or will there be a **contract** in place containing specific data protection clauses* with the organisation(s) you plan to share information with? ** the contract clauses will need to reflect the mitigations identified at Step11 to minimise the data protection risks*	YES ☐	NO ☐

If **NO,** in the absence of a contract what agreement will be in place?

e.g Data Sharing Agreement, Data Access Agreement, Memorandum of Understanding

Please provide details below:

Step 11. IDENTIFY, ASSESS AND MITIGATE ANY DATA PROTECTION RISKS

In this section you are asked to first identify and describe the specific risks associated with this project/process and assess the nature of potential impact on individuals. You will then describe the measures you could take to reduce each identified risk.

To assist you in identifying potential or likely privacy risks you will find a non-exhaustive list of possible risks at Appendix 3.

The **HSC Regional Risk Matrix and Regional Impact Table below** will also help you to assess the level of risk.

	Impact (Consequence) Levels				
Likelihood Scoring Descriptors	**Insignificant (1)**	**Minor (2)**	**Moderate (3)**	**Major (4)**	**Catastrophic (5)**
Almost Certain (5)	**Medium**	**Medium**	**High**	**Extreme**	**Extreme**
Likely (4)	**Low**	**Medium**	**Medium**	**High**	**Extreme**
Possible (3)	**Low**	**Low**	**Medium**	**High**	**Extreme**
Unlikely (2)	**Low**	**Low**	**Medium**	**High**	**High**
Rare (1)	**Low**	**Low**	**Medium**	**High**	**High**

Identify and Assess Risks				Mitigate Risks		
Describe below any specific data protection risks and nature of potential impact on individuals Include <u>associated</u> compliance as necessary *(See Appendix 3 for examples). Please separate your risks out on separate rows*	**Likelihood of occurrence** 1. **Rare** - This will probably never happen/recur 2. **Unlikely** - Do not expect it to happen/recur but it may do so 3. **Possible** - Might happen or recur occasionally 4. **Likely** - Will probably happen/recur, but it is not a persisting issue/circumstances 5. **Almost Certain** - Will undoubtedly happen/recur on a frequent basis **ENTER NUMBERS BELOW**	**Severity of harm (if occurred)** 1. Insignificant 2. Minor 3. Moderate 4. Major 5. Catastrophic	**Overall Risk** **(use Matrix, to calculate overall risk)** Low Medium High	**List the various controls that have been or will be put in place to mitigate the risk prior to commencement** **PLEASE ENSURE YOUR MITIGATION ADDRESSES THE RISK**	**Effect on risk** Reduced Or Accepted* **(***Select 'Accepted' where 'Overall risk' is rated as 'Low')	**Residual risk** Low Medium High
	Choose an item.	Choose an item.	Choose an item.		Choose an item.	Choose an item.

Add additional rows as required. * As per Step 10 please ensure the contract or relevant sharing agreement contains data protection clauses and covers the risks identified above

Step 12. SIGN OFF and record outcomes

a. <u>Project Lead / Service Lead</u>: In signing this DPIA I confirm the following:

I am satisfied that this is an accurate reflection of how the service will be provided and the expected data flows. I have consulted with all necessary stakeholders and sought the views of others as required (including IG and ICT). I have incorporated relevant advice into this document and into the plans for delivery of the service. Where necessary, I will ensure any additional documentation is put in place, such as a Privacy Notice to inform service users of how their personal data is to be processed; and/or any required Contracts or Agreements to cover data sharing with third party organisations.). I will ensure the contract or alternative information sharing agreement will contain specific data protection clauses which address the risks identified.

I confirm that I will keep the DPIA under review and will update this document with any substantive changes to the data processing activities or data flows.

Any additional comments:	
Name and Job Title:	
Signature:	**Date:**

b. Data Protection Officer (DPO) advice and sign-off

Summary of DPO advice:	
Name:	
Signature:	**Date**:

c. Information Asset Owner (IAO) - Final Approval	
I have considered the data protection aspects of this project and any DPO comments (above). I accept any residual risks and will ensure the various controls outlined to mitigate the identified risks are put in place prior to commencement. I will ensure that no data processing will take place until this DPIA has been completed and signed. I will ensure that this DPIA is reviewed and updated if the data processing changes. I will ensure that all staff involved in the processing of personal data are aware of their responsibilities to complete mandatory Information Governance training. I will arrange for this new system/process to be added to the Information Asset Register (IAR) and/or Risk Register.	
Any additional comments:	
Name and Job Title:	
Signature:	**Date**:

Please return a copy of the final signed DPIA to the Information Governance Department

Appendix 1 - Data Protection Principles

The data protection principles are contained in the UK GDPR and require that personal information must be:

a) **Processed lawfully, fairly and in a transparent manner** in relation to the data subject - (Lawfulness, Fairness and transparency). There must be valid grounds under the UK GDPR (known as a 'lawful basis') for collecting and using personal data and you must not do anything with the data in breach of any other laws. Personal data must be processed in a way that is fair and not unduly detrimental, unexpected or misleading to the individuals concerned. You must be clear, open and honest with people from the start about how you will use their personal data.

b) **Collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes. (Purpose limitation)

c) **Adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed - (data minimisation)

d) **Accurate and, where necessary, kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay – (Accuracy)

e) **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed** (Storage Limitation)

f) **Processed in a manner that ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures - (Integrity and Confidentiality)

In accordance with Article 5(2) of the UK GDPR the data controller shall be responsible for, and through its policies, procedures and protocols will demonstrate compliance with the Data Protection Principles listed above **(overarching principle of Accountability).**

Appendix 2 – Lawful Basis for processing Personal Information and Special Category Information

You must have a valid lawful basis in order to process personal data in compliance with Article 6 of UK GDPR.

If you are processing special category data*, you also need to identify a further special category condition in compliance with Article 9 of UK GDPR.

You should document your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability

The lawful bases for processing are set out in **Article 6 of the UK GDPR**. At least one of these must apply whenever you process personal data:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. *(NB. Please consult with your IG Department before using this as your lawful basis for processing personal data. This cannot be applied by a public authority processing data to perform its official / core function (e.g. processing data as part of the provision of health or social care) however may be relevant for non-core functions such as HR)*

Special category data is personal data that needs more protection as it is more sensitive than basic personal data. The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;

- personal data revealing **trade union membership**;
- **genetic data**;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Article 9 lists the conditions for processing special category data:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

See the Information Commissioner's Office (ICO) website (links below):

For more detail on each lawful basis for processing personal data

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

For more detail on the additional conditions for processing special category (sensitive) personal data

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Appendix 3 - Examples of possible risks include: Please note that not all these risks are applicable to every project, nor is this list exhaustive. Please ensure that the risks you list in step 6 are relevant to your project.

DP Principle *(see App 1)*	*Example Risk*	*Example Mitigation*
Lawfulness, Fairness and Transparency	Inadequate Communication – individuals not informed of how the HSC organisation will use their data The form of processing may raise public concerns (e.g. using CCTV footage/audio recording function without informing staff/service users) Privacy notice, consent form, policies and processes not sufficient to cover lawful basis	Privacy Notice in place
		Staff and service users will be informed of the method of data collection and how the data is processed i.e. CCTV/audio recording notification
		Standard operating procedures/staff guidance/ HSC organisation or regional policy/privacy notices and consent forms to be drafted or reviewed in line with the project outcomes
Purpose Limitation	Risk of function creep – that the data is used for a purpose other than the one specified such as using data collected for health for targeted marketing purposes Third party processors/contractors using data for purpose not specified (e.g. marketing purposes)	Clearly defined purpose and limitations set out in information sharing agreement/contract. Review of internal SOP.
		Clearly defined roles and responsibilities included within Contract/Information Sharing Agreement
Data Minimisation	Collecting more data than is required to fulfil purpose	Use of pre-set data fields to ensure no information is collected than necessary
Accuracy:	Mechanisms not in place to ensure data quality/ accuracy to avoid an unintentional data breach or non-compliance.	Ensure all procedures and agreements around data checking are fit for purpose.
	Inappropriate linking/merging records	• Understanding whether system has capacity to link records and if this is appropriate • Ensure there are Data Quality policies and procedures in place

Storage Limitation	Retention – information being retained longer than necessary	• Standard operating procedures to be drafted or reviewed in line with Good Management/ Good Records • Ensure that data retention periods (reflective of GMGR) are outlined in contracts and information sharing agreements and mechanisms exist to manage this by the appropriate parties
	Personal information (manual and electronic records) held with no formal retention policy in place	• Standard operating procedures to be drafted or reviewed in line with Good Management/ Good Records • Ensure that appropriate procedures are in place for retention and disposal of these records
Integrity and Confidentiality (Security)	Risk from threat actors such as cyber criminals, hackers or disgruntled employees on system or cloud	• Use of suitably secure network and file transfer system for transferring information between organisations i.e. Egress. • Consultation with ICT Security re system security. Timely removal of access
	Cyber-attack from unknown source received into the HSC organisation (e.g opening attachment from unknown source which may contain virus)	Consultation with ICT Security team regarding data flows to asses network or system vulnerabilities
	Use of HSC organisation apps on personal devices without a known level of security	Consultation with ICT Security team regarding app/usage vulnerabilities
	Risk when transferring information internally or externally that the information could be inappropriately disclosed during transfer due to inadequate control	Information transferred in line with the HSC organisation's Email Policy i.e. use of secure file transfer system/password protected or encrypted emails

	Unauthorised access to information	• Consultation with ICT Security team re data flows to asses network or system vulnerabilities • Contracts/network access agreements in place • Regular review of systems access holders and prompt removal of access for those no longer requiring it
	Inadequate redaction/anonymisation of data	Checks to be completed on all anonymised/redacted data
	Loss of information due to inadequate controls around tracking/retrieval	• Adhering to data protection policy/guidance • Complying with UKGDPR and Good Management, Good Records to ensure appropriate measures in place to track and retrieve physical documents
	International transfers not monitored resulting information being transferred to servers based in countries without adequacy status or similar DP regime to UK/EU	• Consultation with ICT Security team to identify location of servers and ensure appropriate controls are in place if information will be held in servers outside EEA • Contracts/information sharing agreements will contain clauses governing the transfer of data outside the EEA
	Data loss risk due to system failure	• Back up policies in place • Business continuity measures assessed and in place • Contracts/information sharing agreements to contain clauses governing data loss by 3rd parties
	Intended or accidental linking of data sets that may result in anonymised or pseudonymised data becoming personally identifiable.	• Understanding of whether system has capacity to link records/whether this is appropriate • Data Quality policies and procedures in place

Accountability	Receiving organisation having inadequate framework to support data protection	Assurances to be provided by receiving organisation in the terms of the contract.
CCTV Risks	New surveillance methods may be an unjustified intrusion on privacy	Identify appropriate lawful basis and consult ICO if required to ensure data collection is justified
	Vulnerable people may be particularly concerned about the risks of identification	Appropriate privacy notice in place
	CCTV system is not used for its specified purpose.	• Purpose clearly specified in DPIA/Public Notices • Access to footage limited to only those who require it • Signage in place
	Inability to exercise information rights (e.g. SAR, FOI) if system does not have the functionality to pixelate images which are not the subject.	• Ensure that any surveillance product has the functionality to pixelate or that appropriate contract is in place for adhoc pixilation with a third-party company • Ensure appropriate surveillance policies and processes are in place and that any action taken is compliant
• Data Protection Training is mandatory for every member of HSC staff and should be completed at least every 3 years. Data Protection training will reduce the risks to organisations for non-compliance of UK GDPR and should be considered as an additional mitigating measure for the above-mentioned risks.		