POLICY DOCUMENT

Policy and Procedure for Conducting a Data Protection Impact Assessment

2018 – (Version 1.0)
CS>SMT>G&R>Board

Policy Review Schedule

Date first Approved:

Last Approved by the Board: April 2018

Date of Next Review: April 2020

Policy Owner: Governance, IT & Facilities Manager

Amendment Overview

Version	Date	Pages	Comments	Actioned
2018 – 1.0	04/04/2018		Regionally developed policy adopted and amended to suit NIMDTA.	Mark Oliver
2018 – 1.0	26/04/2018		Presented to NIMDTA Board. **Approved**.	

Contents

Role of the Northern Ireland Medical and Dental Training Agency

The Northern Ireland Medical and Dental Training Agency (NIMDTA) is an Arm's Length Body sponsored by the Department of Health (DoH) to train postgraduate medical and dental professionals for Northern Ireland. NIMDTA seeks to serve the government, public and patients of Northern Ireland by providing specialist advice, listening to local needs and having the agility to respond to regional requirements.

NIMDTA commissions, promotes and oversees postgraduate medical and dental education and training throughout Northern Ireland. Its role is to attract and appoint individuals of the highest calibre to recognised training posts and programmes to ensure the provision of a highly competent medical and dental workforce with the essential skills to meet the changing needs of the population and health and social care in Northern Ireland.

NIMDTA organises and delivers the recruitment, selection and allocation of doctors and dentists to foundation, core and specialty training programmes and rigorously assesses their performance through annual review and appraisal. NIMDTA manages the quality of postgraduate medical and dental education in HSC Trusts and in general medical and dental practices through learning and development agreements, the receipt of reports, regular meetings, trainee surveys and inspection visits. It works in close partnership with local education providers to ensure that the training and supervision of trainees support the delivery of high quality safe patient care.

NIMDTA recognises and trains clinical and educational supervisors and selects, appoints, trains and develops educational leaders for foundation, core and specialty medical and dental training programmes throughout NI.

NIMDTA is accountable to the General Medical Council (GMC) for ensuring that the standards set by the GMC for medical training, educational structures and processes are achieved. The Postgraduate Medical Dean, as the 'Responsible Officer' for doctors in training, has a statutory role in making recommendations to the GMC to support the revalidation of trainees. Revalidation is the process by which the GMC confirms that doctors are up to date and fit to practice. NIMDTA also works to the standards in the COPDEND framework for the quality development of postgraduate Dental training in the UK.

NIMDTA enhances the standard and safety of patient care through the organisation and delivery of relevant and valued career development for general medical and dental practitioners and dental care professionals. It also supports the career development of general medical practitioners and the requirements for revalidation through the management and delivery of GP appraisal.

NIMDTA aims to use the resources provided to it efficiently, effectively and innovatively. NIMDTA's approach to training is that trainees, trainers and educators should put patients first, should strive for excellence and should be strongly supported in their roles.

Executive Summary

A Data Protection Impact Assessment (DPIA) is an assessment of the impact of envisaged data processing operations on the protection of personal data, and particularly an assessment of the likelihood and severity of risks for the rights and freedoms of individuals resulting from this operation. The purpose of this document is to provide guidance on how to assess whether a DPIA is required, and subsequently how to undertake and document a DPIA.

Policy Influence

This policy has been influenced by the following:

- General Data Protection Regulations
- Data Protection Act 1998
- Common Law Duty of Confidentiality
- Computer Misuse Act 1990
- Public Records Act (Northern Ireland) 1923
- Disposal of Documents Order 1925
- Access to Health Records (Northern Ireland) 1923
- Human Rights Act 1998
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Equality Act 2010
- Public Interest Disclosure Act 1998
- The Investigatory Powers Act 2016
- Guidance from the Information Commissioners Office
- The Department of Health (DoH) Good Management, Good Records
- DoH Code of Practice on Protecting the Confidentiality of Service User Information (2012)

Policy Impact

This policy may have an impact on the following:

- Freedom of Information Policy
- Information Requests Procedure
- Freedom of Information Publication Scheme
- Processing and Sharing of Information Relating to Doctors and Dentists
- Data Protection and Confidentiality Policy
- IT Policy
- Records Management Strategy
- Disciplinary Procedure

1. Introduction

A Data Protection Impact Assessment (DPIA) is an assessment of the impact of envisaged data processing operations on the protection of personal data, and particularly an assessment of the likelihood and severity of risks for the rights and freedoms of individuals resulting from this operation.

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

2. Benefits

A DPIA will assist stakeholders in a structured way to identify, categorise and mitigate privacy risks when processing personal data. In addition to the mandatory protection of personal data, a robust DPIA process results in the following:

- Preventing costly adjustments in processes or system redesign by mitigating privacy and data protection risks
- Prevention of discontinuation of a project by early understanding the major risks
- Improving the quality of personal data
- Improving service and operation processes
- Improving decision-making regarding data protection
- Raising privacy awareness
- Improving the feasibility of a project
- Improving communication about privacy and the protection of personal data

3. Purpose

The purpose of this document is to provide 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 data, as well as to assist in the documentation of envisaged safeguards and control measures in proportion to the risks identified. As such, this document shall also be considered integral to the Northern Ireland Medical and Dental Training Agency's (NIMDTA) wider risk management process.

4. Scope

In general, data protection impact assessments are appropriate for projects where one or more of the following applies:

- personal information will be collected and processed for the first time;
- personal information will be shared with people or organisations that previously did not have access to it;
- change of use of existing personal data;
- the use of new technology that processes personal data (e.g. biometrics);
- existing personal data will be used to reach decisions as part of an automated process;
- it might reasonably be expected that an individual may find any aspect of the project intrusive or the data involved private[1];
- processing on a large scale of special categories of data referred to in Article 9(1) of GDPR or of personal data relating to criminal convictions and offences referred to in Article 10 of GDPR;
- datasets that have been matched or combined, which therefore has the potential to identify individuals from previously anonymised / pseudonomised information;
- when the processing in itself 'prevents data subjects from exercising a right or using a service or a contract'

[1] *In the context of this document, the definition of privacy includes the fundamental rights defined in Articles 7 and 8 of the European Union Charter of Human Rights, the right to privacy and the right to the protection of personal data.*

4.1 Format

While GDPR does not prescribe any process or format, a DPIA will contain at least the following:

- a description of the envisaged processing operations and the purposes of the processing, including the legal basis for such;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects that are likely to result from the processing; and,
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR

4.2 When to perform a DPIA

In the case of the development of a new application or system, a DPIA exercise must be carried out from the start of the design and implementation phase, prior to the processing of any personal information. This enables a 'Privacy by Design' approach guaranteeing that potential risks are identified and that appropriate controls can then be incorporated.

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

- significant changes that expand beyond the original purpose(s);
- new types of information processed are introduced;
- unexpected personal data breach with significant impact, the occurrence of which hadn't 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 (e.g. cloud computing)

4.3 Consultation

Appropriate stakeholders must be involved within the development of a DPIA, in order to ensure all of the following aspects are adequately covered:

- Risk assessment
- IT architecture and system engineering
- Information security
- Privacy and data protection
- Organisational design
- Project management

As a minimum, this should include:

- the person(s) in charge of the application / system which is the target of the DPIA;
- person(s) in the design environment, with knowledge of the application / system in question;
- person(s) in the user environment;
- the Data Protection officer (DPO);

In the event that the results of the data protection impact assessment indicate a high level of risk prior to the identified controls being implemented, the GDPR requires that the supervisory authority[2] is consulted before any processing takes place.

5. Conducting the DPIA

5.1 Pre-Assessment

The objective of a pre-assessment questionnaire is to conduct an initial analysis of the system / application / process in question at a 'high level', using a number of criteria to determine whether a full DPIA is required.

[2] *The Information Commissioner's Office (ICO) is United Kingdom's supervisory authority*

This initial questionnaire is set out within the DPIA Pre-Assessment Questionnaire (Appendix 1), and will include the following questions:

- The personal data involved
- Purpose
- Organisational structure / reporting
- Impact on rights / freedoms
- The nature of the applications / system
- Legal basis for processing

5.2 In-depth DPIA

If a determination is made that a more comprehensive DPIA is required, a separate Questionnaire (Appendix 2) will be completed. This will include detailed descriptions of:

- The use of personal data
- Identification, characterisation and description of systems/applications, including data flows
- Identification of relevant risks
- Risk Assessment
- Risk Management
- DPIA Final Report
- Management Approval
- Consultancy with the ICO, if appropriate
- Monitoring / Review

6. Responsibilities

6.1 **The NIMDTA Board** has overall responsibility for effective risk management and this includes oversight of the management of information management within NIMDTA for which the Chief Executive is accountable. The Governance, IT and Facilities Manager has operational responsibility of this policy.

6.2 **Heads of Department** are responsible for ensuring that the policy is fully implemented in their Department and will provide an annual assurance to the Chief Executive Officer that all relevant DPIAs have been conducted within their department on an annual basis.

6.3 **The Data Protection Officer**, under the terms of an SLA with the BSO, will:

- Assist in the production of pre-assessment and DPIA reports;
- Make recommendations and establish mechanisms for review of projects as appropriate

6.4 **All staff** members, whether permanent, temporary or agency are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Staff are expected to familiarise themselves with, and abide by, this policy. Specifically, all staff are responsible for:

- adhering to the requirements within this policy and relevant legislation;
- reporting any relevant incident in line with this policy;
- provision of information and/or reports as requested as part of an investigation;
- taking appropriate action to ensure incidents do not recur

7. Non-Compliance

A failure to adhere to this policy and any associated procedures may result in disciplinary action. In relation to the use of ICT Equipment including the use of the Internet and Email, staff should be aware that they might be personally liable to prosecution if their actions are found to be in breach of the law.

Serious breaches may be reported to the PSNI, ICO or other public authority for further investigation.

8. Review

This policy and any associated procedures will be reviewed initially no later than 1 year from approval, and subsequently no later than every 2 years, to ensure their continued relevance to the effective management of Information Governance within NIMDTA.

9. Equality Statement

In accordance with the, this policy will not discriminate, either directly or indirectly, on the NIMDTA's Equality of Opportunity Policy grounds of gender, race, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, background or any other personal characteristics

Appendix 1

Data Protection Impact Assessment: Screening Questionnaire

This questionnaire is designed to determine whether a more detailed and comprehensive DPIA is required.

Criteria 1: Personal Data Involved

The purpose of this section is to get an initial insight to the data collected

Question	**Yes**	**No**
Will the project involve the collection of new information about individuals?	☐	☐
Will the project compel individuals to provide information about themselves?	☐	☐
Will the personal data be combined with other data from outside the programme/change?	☐	☐
Can the data collected become personal due to linkage by third parties?	☐	☐
Please use this box to supply any further comment in relation to the above		

Criteria 2: Purpose

This section is designed to determine how the information may be used

Question	**Yes**	**No**
Is the purpose of collecting the data clear and shared with the data subjects?	☐	☐
Will the personal data collected be used for any purpose it is not currently used for, or in a way it is not currently used?	☐	☐
Will the data be used for profiling?	☐	☐
Please use this box to supply any further comment in relation to the above		

Criteria 3: The nature of the project

The purpose of this section is to provide a first overview of the application in question. This step will provide an initial insight in the system and potential necessity to carry out a full DPIA.

Question
What is the nature of the application or system?
What components/functions of the application will be considered?

Criteria 4: Responsibilities

The 'owner' of the project needs also to clarify if they can be considered as a data controller or data processor, who conducts the identified processing operations on behalf of the controller.

Question	**Yes**	**No**
Are you defining the conditions and the means of the processing operations (controller)?	☐	☐
Are you conducting the processing on behalf of another organisation (processor)?	☐	☐
Are the roles and responsibilities for ownership and processing of the personal data clear?	☐	☐
Will the processing be handled by a third party processor, or transferred to other organisations who previously did not have routine access to the information?	☐	☐
Please use this box to supply any further comment in relation to the above		

Criteria 5: Impact on rights and freedom

The owner should determine whether the processing presents specific risks to the rights and freedoms of data subjects. The aim is not to conduct a full risk assessment at this stage, but to list the ones which could be already envisaged.

Question	Yes	No
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?[1]	☐	☐
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	☐	☐
Are data subjects able to control which data is collected?	☐	☐
Is it expected that data subjects will change their behaviour due to the fact their personal data will be collected?	☐	☐
Please use this box to supply any further comment in relation to the above		

Criterion 6: Legal basis

The processing of personal data is regulated by GDPR, and the choice of the legal basis for these processing operations has to be carefully selected and justified.

Question	Yes	No
Has the legal basis for the processing of this information been identified?[2]	☐	☐
Please use this box to supply any further comment in relation to the above		

[1] The following can be considered as triggering the need for a full DPIA: Loss of independence; Loss of equality; Stigmatization; Loss of freedom to move; Interference with private life; Manipulation; Loss of Autonomy

[2] The legal basis for processing of personal information is set out within

- Article 6 of GDPR: https://gdpr-info.eu/art-6-gdpr/
- Article 9 of GDPR ('special categories'): https://gdpr-info.eu/art-9-gdpr/

Screening Decision

This section should be completed by the Organisation's Data Protection Officer, in conjunction with other staff as deemed appropriate. A documented conclusion should be produced based upon the answers to the questions. This should be endorsed by the management regarding whether a DPIA is needed or not.

Question	**Yes**	**No**
Is there sufficient information to make an informed decision on whether a full DPIA is necessary?	☐	☐
In consideration of the information supplied, is a full DPIA required?	☐	☐
Please use this box to supply any further comment in relation to the above		

Appendix 2

Data Protection Impact Assessment: Northern Ireland Medical and Dental Training Agency (NIMDTA)

Project Title:

Document Version

Date	Version	Description

Contents

Section 1: Background Information; Aims and Objectives

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 Data Protection Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a DPIA 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	☐	
	Physical description	☐	
	NHS no.	☐	
	Mobile/home phone no.	☐	
	Email address	☐	
	Other, specify	☐	

Sensitive classes of information (GDPR, Article 9)	Yes	N/A	**Justification**
Information revealing revealing racial or ethnic origin	☐	☐	
Information revealing revealing political opinions	☐	☐	
Information revealing revealing religious or philosophical beliefs	☐	☐	
Information revealing trade union membership	☐	☐	
Genetic and/or biometric data to uniquely identify a natural person	☐	☐	
Information concerning health	☐	☐	
Information revealing sex life or sexual orientation	☐	☐	
personal data relating to criminal convictions and offences or related security measures	☐	☐	

Section 3: Business Process Flow

Flow chart

Section 4: Assessment

	Question	Response	Required Action **E.g. Seek Information Governance advice**
Processed lawfully, fairly and in a transparent manner in Relation to individuals	1. What is the legal basis for processing the information? *This should include which conditions for processing under Data Protection legislation apply and the common law duty of confidentiality.*		
	2. 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?		
	3. 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?		
	4. 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	5. Does the project involve the use of existing personal data for new purposes?		
	6. Are potential new purposes likely to be identified as the scope of the project expands?		
Adequate, Relevant	7. 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	8. Are you able to amend information when necessary to ensure it is up to date?	Yes	
	9. How are you ensuring that personal data obtained from individuals or other organisations is accurate?		
Retention	10. What are the retention periods for the personal information and how will this be implemented?		
	11. Are there any exceptional circumstances for retaining certain data for longer than the normal period?		
	12. How will information be fully anonymised or destroyed after it is no longer necessary?		
Rights of the individual	13. 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	14. What procedures are in place to ensure that all staff with access to the information have adequate information governance training?		
	15. If you are using an electronic system to process the information, what security measures are in place?		
	16. How will the information be provided, collate, used and stored?		
	17. What security measures will be used to transfer the identifiable information?		
Transfers both internal and external including outside of the EEA	18. Will individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?		
	19. 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	20. 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.*		
	21. 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	22. List any national guidance applicable to the initiative that is referred to.		

Section 5 – Privacy issues identified and risk analysis

a) 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	**(a) Risk to individuals** *(complete if appropriate to issue or put not applicable)*	**(b) Compliance risk** *(complete if appropriate to issue or put not applicable)*	**(c) Associated organisation/corporate risk** *(complete if appropriate to issue or put not applicable)*

b) 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**			

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**		

Section 6: DPIA Report

- The evaluation of all of the above will result in the production of the data protection impact assessment report which will summarise:
- A description of the proposed processing operations and the personal data involved
- The purposes of the processing including, the legal basis as defined by the GDPR
- An assessment of the necessity and proportionality of the processing
- The results of the assessment of the risks to the rights and freedoms of the data subjects
- Whether consultation with the ICO is necessary
- The need, or otherwise to review the DPIA (and appropriate timescales for doing so)
- Overall acceptance of the project, or otherwise

Signature of reviewer:

Role:

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 Data Protection Act 1998
- 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.