**Data Protection Impact Assessment**

**Policy**

**Document Control:**

|  |  |
| --- | --- |
| **Version** | 1.0 |
| **Name and designation of policy author(s)** | Dr. Murugesh VelayudhamGP Senior Partner |
| **Ratified by** | Deepa Gnanasundaram |
| **Date Ratified** | March 2024 |
| **Responsible Committee/Officers** | Data Protection Officer/Data Processing Officer/ |
| **Date Issue** | 20/02/2024 |
| **Review Date** | Feb 2025 |
| **Intended Audience** | Practice Staff and Patients |
| **Links to other strategies, policies, procedures** | Access to Health Records Act 1990 |

**Version History:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Author name and designation** | **Summary of main changes** |
| **Feb 2024** | **1.0** | **Dr. Murugesh Velayudham** GP Senior Partner |  |

**Table of Contents**

[**1.** **Introduction** 4](#_Toc157064948)

[**2.** **Purpose** 4](#_Toc157064949)

[**3.** **Scope** 4](#_Toc157064950)

[**4.** **Responsibilities** 5](#_Toc157064951)

[**5.** **Definitions** 6](#_Toc157064952)

[**6.** **Laws & Regulations** 7](#_Toc157064953)

[**7.** **Data Protection Impact Assessment Requirements** 7](#_Toc157064954)

[7.1 Identifying the need for a DPIA 7](#_Toc157064955)

[7.2 Undertaking a DPIA 8](#_Toc157064956)

[7.3 Consultation with the Information Commissioner’s Office (ICO) 9](#_Toc157064957)

[7.4 Review of DPIAs 9](#_Toc157064958)

[7.5 Disclosure and publication of DPIAs 10](#_Toc157064959)

[**8.** **Review of the Policy** 10](#_Toc157064960)

[**Appendix A** 11](#_Toc157064961)

# **Introduction**

* 1. Protecting the confidentiality of individuals and not infringing on data subjects privacy has become a much larger consideration for the public sector in recent decades, and with the development of new technologies this has increased public concerns about intrusion into their privacy.
	2. It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA). However, the UK General Data Protection Regulations (UK GDPR) makes privacy by design an expressed legal requirement, under the term ‘data protection by design and by default’. Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. The Practice will implement appropriate technical and organisational measures to show that it has considered and integrated the principles of data protection into its processing activities. The UK GDPR also makes PIAs – referred to as ‘Data Protection Impact Assessments’ or DPIAs – mandatory in certain circumstances.
	3. Data Protection Impact Assessment (DPIA) are a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. DPIAs help identify privacy risks, foresee problems and bring forward solutions.

# **Purpose**

* 1. The purpose of this policy is to ensure that risks to the rights and privacy of individuals are minimised while allowing the aims of the new/changed processing operations to be met whenever possible.
	2. This policy provides a standardised approach towards identifying, assessing and mitigating data protection and privacy risk and assists towards the delivery of compliance with legal statutory requirements.
	3. Risks can be identified and addressed at an early stage by analysing how the proposed uses of data, technology and processes will work in practice. This analysis can be tested by consulting with the stakeholders who will be working on, or affected by, the new/changed processing operation.

# **Scope**

* 1. This document applies to those members of staff that are directly employed by the Practice and for whom the Practice has legal responsibility, as well as any Processors/contractors/sub-contractors/third parties processing Practice data or accessing systems, or anyone authorised to undertake work on behalf of the Practice. For those staff covered by a letter of authority/honorary contract or work experience, the organisation’s policies are also applicable whilst undertaking duties for or on behalf of the Practice.

# **Responsibilities**

* 1. **Senior Information Risk Owner**

The Senior Information Risk Owner (SIRO) is accountable for information risk within the Practice. The Practice’s SIRO is Dr. Murugesh Velayudham, the GP senior partner.

* 1. **Caldicott Guardian**
		1. The Caldicott Guardian has responsibility for overseeing the implementation of the laws that govern personal information and ensuring that good practice in relation to access and reuse of data is implemented within the Practice.

The Caldicott Guardian is the Practice champion in respect of the Caldicott Principles and as such is obligated to always make Caldicott decisions in the best interests of the patient. The Practice’s Caldicott Guardian is Deepa Gnanasundaram, the Practice Manager.

* 1. **Data Protection Officer**
		1. The Data Protection Officer (DPO) has responsibility for informing and advising and monitoring compliance with data protection principles. The DPO for the Practice is held by the NHS Informatics Merseyside Data Protection Officer as a Service.
		2. The DPO will:
* Provide advice to the Practice and its employees on compliance obligations with data protection law
* Advise on when data protection impact assessments are required
* Monitor compliance with data protection law and organisational policies in relation to data protection law
* Co-operate with, and be the first point of contact for the Information Commissioner
* Be the first point of contact within the organisation for all data protection matters
* Be available to be contacted directly by data subjects
* Take into account information risk when performing the above
	1. **All Staff**
		1. It is the responsibility of all staff to:
* Adhere to this policy
* To know where to access further support
* Complete annual Data Security Awareness mandatory training

# **Definitions**

* 1. **Personal Data**

Personal Data is any information relating to an identifiable person who can be directly or indirectly identified:

* Key identifiable information includes:
* Person’s name, address, full post code, date of birth;
* Pictures, photographs, videos, audio-tapes or other images of a person;
* NHS number and local patient identifiable codes;
* Anything else that may be used to identify a person directly or indirectly e.g. rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.
	1. **Special Categories of Personal Data (Sensitive Data)**

Data held about an individual which contains both personal and sensitive information. Information categories detailed in the UK General Data Protection Regulations that are deemed as special categories of personal data:

* Racial or ethnic origin;
* Religious or philosophical beliefs;
* Political opinions;
* Trade union membership;
* Genetic data (for the purpose of uniquely identifying a person);
* Biometric data (for the purpose of uniquely identifying a person);
* Physical or mental health;
* Sexual life/sexual orientation
	1. **Data Controller**

A ‘Data Controller’ is: a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

* 1. **Data Processor**

A ‘Data Processor’ is: any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.

* 1. **Data Subject**

A ‘Data Subject’ means an individual who is the subject of personal data and must be a living individual.

* 1. **Processing**

‘Processing’, in relation to information or data, means: obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, whether or not by automated means, including:

* collection
* recording
* organisation
* structuring
* storage
* adaptation or alteration
* retrieval
* consultation
* use
* disclosure by transmission,
* dissemination or otherwise making available
* alignment or combination
* restriction
* erasure or destruction
1. **Laws & Regulations**
	1. This Data Protection Impact Assessment Policy will ensure that the Practice complies with all relevant laws, legislation and regulation. This will include (but is not limited to):
* [Data Protection Act 2018](https://www.gov.uk/data-protection)
* [UK General Data Protection Regulations (UK GDPR)](https://www.legislation.gov.uk/eur/2016/679)
* [Health & Social Care Act 2012](https://www.legislation.gov.uk/ukpga/2012/7/contents)
* [Common Law Duty of Confidentiality](https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care/hscic-guide-to-confidentiality-references/section-2)
* [Confidentiality: NHS Code of Practice](https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice)
* [Records Management Code of Practice for Health and Social Care 2021](https://transform.england.nhs.uk/media/documents/NHSX_Records_Management_CoP_V7.pdf)

# **Data Protection Impact Assessment Requirements**

## **Identifying the need for a DPIA**

* + 1. A DPIA must be undertaken before the processing of any personal data which is “likely to result in a high risk to the rights and freedoms” of individuals. As such, it is necessary to identify whether there are any factors that warrant the need for a DPIA to be undertaken.
		2. A DPIA must be considered in the following circumstances:
* Introduction of a new paper or electronic information system for storing and accessing personal data.
* Update or revision of a key system that might alter the way in which the practice uses, monitors and reports personal data.
* Changes to an existing system where additional personal data will be collected
* Proposal to collect personal data from a new source or for a new activity
* Using existing data for a new and unexpected or more intrusive purpose
* Plans to outsource business processes involving storing and processing personal data
* Plans to transfer services from one provider to another that include the transfer of information assets
* Changes to or introduction of new information sharing agreements
* A new surveillance system
	+ 1. Where there is new or changed processing of personal data, the DPIA Screening section in ***Appendix A*** should be completed. It is expected that the screening will be completed by Deepa Gnanasundaram, the Practice Manager.
		2. Before completing the DPIA Screening, it is important to:
* identify the key stakeholders in the new or changed processing of personal data so that they can provide their input into the DPIA Screening
* have a clear understanding of the scope and objectives of the new or changed processing of personal data so that the DPIA Screening can be completed as fully and accurately as possible
	+ 1. If there is any uncertainty regarding completion of the DPIA Screening or the outcome, the NHS Informatics Merseyside Data Protection Officer as a Service Team should be consulted.
		2. Where the outcome of the DPIA Screening suggests that the processing is unlikely to result in a high risk to individuals, there may be circumstances where it is advisable to undertake a DPIA anyway due to:
* the nature, scope, context and purposes of processing personal data
* the groups of individuals affected by the processing (e.g. children or vulnerable adults)
* the level of investment in the new or changed processing of personal data in terms of time, financial and other resources
* the visibility of the new or changed processing of personal data internally and externally
	+ 1. Where the DPIA Screening has concluded that a full DPIA is unnecessary and will not be undertaken, the reasons for this should be clearly documented with approval from DPO, Caldicott Guardian and SIRO. The DPIA Screening should be retained to evidence the decision made and may need to be revisited and reviewed at a later date.

## **Undertaking a DPIA**

* + 1. Where the DPIA Screening has concluded that a full DPIA is necessary or desirable for a particular new or changed processing of personal data, the full DPIA section in ***Appendix A*** should be completed. The full DPIA Template explains the objectives and requirements of each section. Where any section is not completed because it is not applicable or not considered necessary, this should be explained.

## **Consultation with the Information Commissioner’s Office (ICO)**

* + 1. Where the outcome of a full DPIA is that the processing of personal data in would result in a high risk and it is not possible to take any measures to eliminate or mitigate to reduce that risk, UK GDPR requires that the processing cannot commence before the ICO has been consulted.
		2. The ICO should not be consulted direct by the Practice, the NHS Informatics Merseyside Data Protection Officer as a Service

 will usually initiate contact with the ICO. Consultation with the ICO should only be necessary in very exceptional instances as it is expected that the Practice will be able to apply measures to appropriately mitigate or eliminate risk on most occasions.

* NHS Informatics Merseyside Data Protection Officer as a Service will contact the ICO via dpiaconsultation@ico.org.uk sending:
* a copy of the DPIA
* a cover letter
* the purposes and methods of the intended processing
* the measures and safeguards taken to protect individuals
* a description of the respective roles and responsibilities of any joint controllers or processors DPO contact details
	+ 1. The ICO intends to respond to requests for consultation within eight weeks, though it can extend such period by a further six weeks in complex cases.
		2. The ICO will provide a written response confirming whether the risks identified are acceptable or whether further action is required. In some cases, the ICO may recommend that the processing is not undertaken.

## **Review of DPIAs**

* + 1. A DPIA should be undertaken at the earliest opportunity in the development of the new or changed processing of personal data and re-assessed prior to commencement of the relevant processing activities to identify whether any changes impact upon the outcomes of the DPIA and whether the controls and measures identified in the DPIA have been integrated into the new or changed processing of personal data.
		2. Once the new or changed processing of personal data has commenced, the DPIA should be reviewed regularly having regard to the nature and risks associated with the processing, taking into account any changes to the processing activities or scope. A review should be undertaken at least annually by Dr. Murugesh Velayudham, GP Senior Partner.

## **Disclosure and publication of DPIAs**

* + 1. There is no legal requirement to proactively disclose or publish a DPIA, although it could be subject to a request made under the Freedom of Information Act 2000 so may need to be released, subject to any exemptions contained in the legislation. However, it may be necessary to disclose a DPIA to another institution to provide assurance that due and proper consideration has been given to the data protection implications of an initiative.
1. **Review of the Policy**
	1. This policy will be reviewed every annual year, by Deepa Gnanasundaram, the Practice Manager.

# **Appendix A**

**Data Protection Impact**

**Assessment (DPIA) Template**

Making exceptional service the standard

****

|  |
| --- |
| **Data Protection Impact Assessment (DPIA)** |
| This assessment should be completed as part of the business case for all new information systems / processes / projects which involve the use of personal sensitive data or will significantly change the way in which personal data is handled. |
| The DPIA should be sent to Caldicott Guardian/IG Lead/SIRO for review and approval DPO advice may be useful at any stage, including:* how to complete a particular section of the form
* whether a full DPIA is necessary (Screening section)
* possible measures and safeguards to mitigate risks.

The DPO must review the completed form and advise on whether processing should go ahead. |
| **General Details** |
| 1 | Name of the new system / process / project |  |
| 2 | Person completing this assessment:  | Name: Job Title: Email:  |
| 3 | Date completed |  |
| 4 | Background:*(Why is the new system/change required - The purpose and aims of this work.)* |  |
| 5 | What are the main aims?*(Why is it needed, what is it aiming to achieve, what is the business rationale for it, etc?)* |  |
| 6 | List the main activities of the project: |  |
| 7 | What are the intended outcomes? |  |
| 8 | (Anticipated) Go-Live Date:  |  |
| 9 | Information Asset Owners (All system/assets must have Information Asset Owners (IAO). IAO’s will be the Practice Manager or Partner GP *This is the person who takes overall responsibility for this asset and may do so for several other assets. The IAO is responsible for reporting any breaches that happen with their assets to the SIRO, as well as identifying and mitigating any risks to the asset, and deciding which users have access to it.* | Name: |  |
| Title: |  |
| Department: |  |
| Telephone: |  |
| Email: |  |
| 10 | Who is the Information Asset Administrator?*The IAA is an operational staff member who has day to day responsibility for ensuring that the asset is secure and that those who should be able to access it are able to do so*. | Name: |  |
| Email: |  |
| **DPIA Screening** |
| Screening Questions | Yes/No | Comments |
| A | Will the project involve the collection of new information about individuals?  |  |  |
| B | Will the project compel individuals to provide information about themselves?  |  |  |
| C | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? |  |  |
| D | Do you propose using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?  |  |  |
| E | Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition |  |  |
| F | Will the project result in you making decisions or acting against individuals in ways which can have a significant impact on them? *(e.g., service planning, commissioning of new services ect.)* |  |  |
| G | Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? e.g., health records, criminal records or other information that people would consider to be particularly private?***(N.B.*** *If the project is using anonymised/pseudonymised data* ***only****, the response to this question is “****No****”.)* |  |  |
| H | Will the project require you to contact individuals in ways which they may find intrusive? |  |  |
| I | Will the project store information using cloud technology? |  |  |
| J | Will the project transfer information outside the UK?  |  |  |
| * If you answered “**No”** to all the questions, you **DO NOT** need to proceed to a full DPIA. Save this document to evidence your assessment
* If you answered “**Yes”** to any of these questions, you **DO** need to proceed to a full DPIA. Complete the rest of the document, forward to appropriate persons for review and approval and save to evidence your assessment
* If, however, you answered “**Yes**” to any of the questions, but feel it is not necessary to complete the full DPIA, please provide the justification for this below and send to appropriate persons for review and approval and save to evidence your assessment.
 |
| K | Justification |  |
| **Full Data Protection Impact Assessment**  |
| 11 | Who are the Data Subjects? *(The people whose data will be held/processed in this new system – this may be patients, staff and/or other individuals)* |  |
| 12 | What Data Classes will be held on this system *(The actual data fields) split by Personal and Special Category)* | Personal Data: |
| Special Category Data:  |
| 13 | Children (those under 13 years of age): does the project involve internet services of any kind, with regards to children?  |  |
| 14 | If yes, are you planning to gain and record consent? How will you achieve this?  |  |
| 15 | If the child is under 13 years of age, will you gain and record the parents’ consent? If Yes, how will you achieve this? |  |
| 16 | Who will be the data controller(s)? |  |
| 17 | Will there be any data processors/sub-processors? |  |
| 18 | Will this system/process include data which was not previously collected? |  |
| 19 | Have you assessed the likelihood of data causing any unwarranted distress or damage to individuals concerned? |  |
| 20 | Is there a legal basis for holding and processing this data?*(Need to identify UK GDPR Article 6 basis for any personal data and UK GDPR Article 9 basis for any special category data.)* | Article 6(1) Lawfulness of processing: |
| Article 9(2) Processing of special categories of personal data:  |
| 21 | How does this comply with the Common Law Duty of Confidentiality? |  |
| 22 | Does the system/process include new or amended identity authentication requirements that may be intrusive? |  |
| 23 | What checks have been made regarding the adequacy, relevance and necessity of data used? |  |
| 24 | Can the system/process use pseudonyms or work on anonymous data? |  |
| 25 | Can the data subjects opt-out of their data being added to the system/used by the process, and if so, is this publicised? |  |
| 26 | Does the Fair Processing Notice (or Privacy Notice on the practice’s public website cover your planned activity |  |
| 27 | Who are the partners for the data sharing? |  |
| 28 | Is there an information sharing agreement or is one needed? |  |
| **Data Security** |
| 29 | Will the system require the use of the practice computer equipment? If so, has the Informatics Merseyside (IM) IT Security Team been informed and assessed the system?  | . |
| 30 | Who will use the system/process and have access to the data? |  |
| 31 | Have or will areas involved completed the Data Security Awareness Level 1 eLearning module |  |
| 32 | What other, if any, training will users receive? |  |
| 33 | Will the data be shared with any other organisations?*(check privacy policy of provider/Sharing Agreements for details)* |  |
| 34 | Where will data be held?  |  |
| 35 | What format will data be stored in? |  |
| 36 | Does the system / process change the way data is stored? |  |
| 37 | How will staff access and amend data? |  |
| 38 | How will data be shared? *(e.g., email, NHS mail, internal/external post, phone, website transfer, mesh, sms, secure systems)* |  |
| 39 | Are you transferring any personal and / or sensitive data to a country outside the UK? | [ ]  Yes [ ]  No*If yes, please outline the data types, country, transfer methods and any measures in place to ensure adequate levels of security when transferred to this country. Have Standard Contractual Clauses been used?* |
| 40 | Give a description of all information flows (or diagram)  |  |
| 41 | What security measures have been taken to protect the data? *(request 3rd party security whitepapers or documentation for system)**Please include access control, data security in transit and encryption in the answer*  |  |
| 42 | Is there a useable audit trail in place for the asset? *(e.g. to identify who has accessed a record)* |  |
| 43 | How often will the system/process be audited? |  |
| 44 | Who supplies the system/process? |  |
| 45 | If the supplier is third party, are they based within the UK *(if “No”, give details of base)*  |  |
| 46 | Where will the supplier store the data? *(Give full address(es).)*  |  |
| 47 | Is the supplier of the system/recipient of the data registered with the ICO? *(give registration number(s).)* |  |
| 48 | Has the organisation completed the Data Security and Protection Toolkit (DSPT) to a satisfactory level? *(Give the organisational code)* |  |
| 49 | Does the contract include Data Protection clauses? |  |
| 50 | If “No”, is a Data Processor Contract required? |  |
| 51 | What business continuity plans are in place? *(e.g. in the case of data loss/damage because of: human error, computer virus, network failure, theft, fire, flood,etc)**(for the practice)* |  |
| **Data Quality**  |
| 52 | Who provides the information for the asset? |  |
| 53 | Who inputs the data into the system?  |  |
| 54 | How will the information be kept up to date and checked for accuracy and completeness? |  |
| 55 | Can an individual (or a court) request amendments or deletion of data from the system? |  |
| **On-Going Use of Data** |
| 56 | Will the data be used to send direct marketing messages?  |  |
| 57 | If yes, are consent and opt-in procedures in place? |  |
| 58 | Does the system/process change the medium for disclosure of publicly available information? |  |
| 59 | Will the system/process make data more readily accessible than before? |  |
| 60 | What is the data retention period for this data? *(please refer to* [*Records Management Code of Practice 2021*](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/)*)* |  |
| 61 | How will the data be destroyed when it is no longer required? |  |
| 62 | Does your disaster recovery solution use a third-party supplier? |  |
| 63 | Does your Disaster recovery provider have any accreditations? e.g., ISO27001 |  |
| 64 | Has your Disaster Recovery Plan been tested and was all data retained and secure? |  |
| **Identify and Assess Risks**  |
| Information security risks should be highlighted to the IM IT Security Team to complete any necessary risk assessments on new systems or changes to existing systems. Any issues that may arise could adversely impact other organisations and services hosted by Informatics Merseyside, because of this the IM IT Security Team need to complete their assessment before the system can be commissioned for use.  |
| 65 | **Risk Description (**source of risk and nature of potential impact **to individuals, the Practice, CCG or to wider compliance)** | **Likelihood of harm**(Remote, possible or probable) | **Severity of harm**(minimal, significant or severe) | **Overall risk**(low, medium or high) |
| A |  |  |  |  |
| B |  |  |  |  |
| **Identify Measure to Reduce Risk** |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in the table above** |
| 66 | **Proposed Risk Solution** (reduce or eliminate risk) | **Effect on risk**(Is the risk reduced, transferred, accepted) | **Remaining risk**(Low, medium or high) | **Measure approved**(Yes/No) |
| A |  |  |  |  |
| B |  |  |  |  |
| **DPIA Sign Off** |
| Item | Name/Date | Notes  |
| SIRO approved: | Name: | *Integrated actions back into project plan, with date and responsibility for completion* |
| Date: |
| Caldicott Guardian approved:  | Name:  | *If accepting any residual high risk, consult the ICO before going ahead* |
| Date: |
| DPO advice provided  | Name:  | *DPO should advise on compliance, identify measure to reduce risk section and whether processing can proceed* |
| Date:  |
| Summary of DPO advice:  |
| DPO advice accepted or overruled by:(SIRO/Caldicott Guardian) | Name: | *If overruled, you must explain your reasons* |
| Date: |
| Comments: |
| Consultation responses reviewed by: | Name: | *If your decision departs from individuals’ views, you must explain your reasons* |
| Date: |
| Comments: |
| This DPIA will be kept under review by: | Name: | *The DPO should also review ongoing compliance with DPIA* |
| Date: |