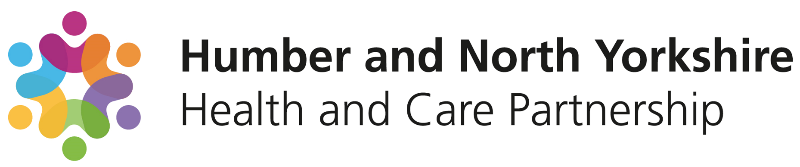
****

**Data Protection by Design & Default Policy and Procedure**

**Completion of Data Protection Impact Assessments**

**February 2024**

|  |  |
| --- | --- |
| **Authorship:** | Information Governance Officer |
| **Committee Approved:** | Senior Information Risk Owner |
| **Approved date:** | February 2024 |
| **Equality Impact Assessment:** | November 2023 |
| **Target Audience:** | ICB and its Committees and Sub-Committees, ICB Staff, agency, and temporary staff & third parties under contract |
| **Policy Number:** | ICB64 |
| **Version Number:** | 1.0 |

**The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as ‘uncontrolled’ and as such may not necessarily contain the latest updates and amendments.**

**AMENDMENTS**

Amendments to the policy may be issued from time to time. A new amendment history will be issued with each change.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **New Version Number** | **Issued by** | **Nature of Amendment** | **Approving body** | **Approval date** | **Date published on website** |
| 1.0 | Executive Director of Corporate Affairs | New Policy for ICB | SIRO | 09.02.24 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Contents

[1 Introduction 4](#_Toc155086002)

[1.1 Data Protection by Design and Default 4](#_Toc155086003)

[1.2 Data Protection Impact Assessments 4](#_Toc155086004)

[2 Purpose 4](#_Toc155086005)

[3 Scope of the Policy 5](#_Toc155086006)

[4 Definition/ Explanation of Terms 5](#_Toc155086007)

[4.1 Pseudonymisation 5](#_Toc155086008)

[4.2 Information Asset Register and Data flows 5](#_Toc155086009)

[4.3 Common Law Duty of Confidentiality 6](#_Toc155086010)

[4.4 UK GDPR 6](#_Toc155086011)

[4.5 Data Sharing Agreements 6](#_Toc155086012)

[4.6 Privacy Enhancing Technologies 6](#_Toc155086013)

[5 Duties/ Accountabilities and Responsibilities 6](#_Toc155086014)

[5.1 Duties within the organisation 6](#_Toc155086015)

[5.2 Chief Executive 7](#_Toc155086016)

[5.3 Caldicott Guardian 7](#_Toc155086017)

[5.5 Data Protection Officer (DPO) 7](#_Toc155086018)

[5.6 Senior Information Governance Manager 8](#_Toc155086019)

[5.7 Information Asset Owners & Administrators (IAOs & IAAs) 8](#_Toc155086020)

[5.8 Line Mangers 8](#_Toc155086021)

[5.9 All staff 9](#_Toc155086022)

[5.10 Responsibilities for approval 9](#_Toc155086023)

[6 Consultation 9](#_Toc155086024)

[7 Training 9](#_Toc155086025)

[8 Monitoring Compliance 9](#_Toc155086026)

[9 Arrangements for Review 9](#_Toc155086027)

[10 Dissemination 9](#_Toc155086028)

[11 Associated Documentation 9](#_Toc155086029)

[12 References 10](#_Toc155086030)

[13 Policy Document Requirements 11](#_Toc155086031)

[13.1 Why do I need to complete a DPIA? 11](#_Toc155086032)

[13.2 Is a DPIA required for every project? 12](#_Toc155086033)

[13.3 When Should I Start a DPIA? 12](#_Toc155086034)

[14 Impact Assessments 13](#_Toc155086035)

[14.1 Equality 13](#_Toc155086036)

[14.2 Bribery Act 2010 13](#_Toc155086037)

[14.3 General Data Protection Regulations (GDPR) 13](#_Toc155086038)

[15 Appendices 14](#_Toc155086039)

[15.1 Appendix 1 - The DPIA Procedure 14](#_Toc155086040)

[15.2 Appendix 2 - Anti-Fraud, Bribery and Corruption 15](#_Toc155086041)

[15.3 Appendix 3 – DPIA Template 17](#_Toc155086042)

# Introduction

## 1.1 Data Protection by Design and Default

It is a requirement of UK GDPR to implement appropriate technical and organisational measures to embed the data protection principles effectively, and to safeguard individual rights. It is essential to integrate data protection into all processing activities and operational practices from the design stage through the lifecycle of each and every project. This is known as Data Protection by Design and Default.

Data Protection by Design and Default has a broad application and is supported through the implementation of organisational policies, data sharing initiatives, staff training, privacy-enhancing technologies, risk anticipation, Data Protection Impact Assessments (DPIA), and a dedicated Information Governance team. Other measures include tracking the flow of organisational data and ownership of assets, etc. via the Information Asset Register (IAR) and Data Flow Mapping.

## 1.2 Data Protection Impact Assessments

The Information Commissioner’s Office has increased powers of audit within organisations and can fine organisations up to £17.5 million or 4% of the annual worldwide turnover, whichever is higher, for not having appropriate procedures in place to manage the use of personal identifiable information.

Data Protection Impact Assessments (DPIAs) are required under UK GDPR legislation, where health data is being used in a manner that it either is identifiable or there is a risk of an individuals’ identity being revealed. A DPIA should also be considered where other personal data, for example data about individual staff, is being used in a way that could poses a high level of risk regarding the privacy of those individuals.

DPIAs aid organisations in determining how a particular project, process or system may affect the privacy of the individual. This procedure consists of DPIA Screening Questions and Data Protection Impact Assessment which are designed to enable an assessment prior to new services or new data processing/sharing systems being introduced. A DPIA is not effective when key decisions have already been taken. If an assessment is suggested, it should be seen as dynamic and subject to review with any significant change.

DPIAs identify the most effective way to comply with data protection obligations and meet individuals’ expectations of privacy. An effective DPIA will allow for the identification and remedy of problems at an early stage, reducing potential distress, subsequent complaints and the associated costs and damage to reputation that might otherwise occur.

It is important to consider whether a DPIA is required as soon as the objectives/aims of the project are identified to examine what is required to successfully meet these and how it is envisaged this will happen, whilst ensuring privacy of individuals to which the data relates.

Conducting a DPIA should not be complex or time consuming if it is given due regard at an early stage.

# Purpose

The purpose and objectives of this policy and procedure are to ensure the HNY ICB comply with Data Protection legislation, and to protect the ICB along with its service users, patients, staff, and other stakeholders, as well as the assets of the ICB, whilst ensuring delivery of its strategic and corporate objectives.

The ICB believes that individuals have a right to privacy and confidentiality and will ensure that this policy supports the common law duty of confidentiality and statutory provisions that prevent unlawful sharing of personal information. The processing of such information will be dealt with under and in compliance with the provisions of current data protection legislation.

The ICB must carry out its duties effectively and lawfully and ensure the exemptions and exceptions outlined in the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 will be applied appropriately.

# Scope of the Policy

The policy applies to all ICB employees and all who work for the organisation, including the Governing Body, contracted third parties including temporary agency or honorary contracts, secondments, pool staff, contractors, students, and trainees.

Failure to comply with this policy will be considered in breach of the terms and conditions of employment and may be treated as a disciplinary offence under the ICB's disciplinary procedure.

# Definition/ Explanation of Terms

## Pseudonymisation

Pseudonymisation involves the removing of identifiers from patient data so that patient/service user may not be identified. The aim of pseudonymisation (vs anonymisation) is to be able to collect additional data relating to the same individual without having to know the identity so that it is possible, for example, to analyse data sets and trends over time. Individual service user activity should be able to be identified but not the service user themselves. This will often be achieved by attaching codes or other unique references to information so that the data will only be identifiable to those who have access to the key or index.

Under Data Protection legislation, information that has been pseudonymised can still be considered as identifiable (and therefore within the remit of the legislation)

Before personal information is processed within the ICB, staff must consider whether the purpose can be achieved with anonymised or pseudonymised information.

## Information Asset Register and Data flows

The Information Asset Register is a register of personal and business critical information held by the ICB. It details the type of information held, purpose, legal basis, location, sharing arrangements, associated risks and other detailed information.

Data flow mapping is a process which helps the organisation understand what information it receives, where it is held and how it is transferred. Flows of personal or potentially identifiable information should be documented on the ICB’s data flow template.

More information can be found in the Information Asset Owner’s Handbook.

## Common Law Duty of Confidentiality

The so-called *common law duty of confidentiality* is complex: essentially it means that when someone shares personal information in confidence it must not be disclosed without some form of legal authority or justification. In practice this will often mean that the information cannot be disclosed without that person’s explicit consent unless there is another valid legal basis. It is irrelevant whether the individual has mental health issues or indeed lacks capacity: the duty still applies.

## UK GDPR

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses, or the government.

The Data Protection Act 2018 is the UK’s implementation of the General Data Protection Regulation (GDPR).

## Data Sharing Agreements

A Data Sharing Agreement (DSA) or Information Sharing Agreement (ISA) is a document which details the data sharing arrangement between organisations. It will describe which organisations are involved, their purpose for sharing or processing data, and their legal basis for doing so. A DSA should show that you have been mindful of potential compliance issues and justify the need to share data. A DSA compliments a DPIA and assists an organisation to comply with data confidentiality law and legislation.

## Privacy Enhancing Technologies

Privacy Enhancing Technologies (PET’s) are software and hardware solutions that are employed with the specific purpose of protecting the data and privacy of service users digitally. PETs are linked to the concept of *‘data protection by design and default’* and aid the integration of data protection safeguards in the technological and systemic operations of organisations.

# Duties/ Accountabilities and Responsibilities

## Duties within the organisation

Responsibility for ensuring that a Data Protection Impact Assessment is considered and, where appropriate, completed resides with the manager(s) leading the introduction of new systems, data sharing or projects. Completion of the Screening Questions also serves to evidence that this has been considered.

There is an expectation that partner organisations/third parties involved in supplying/providing services will contribute the necessary technical information for the Data Protection Impact Assessment.

This guidance therefore applies to all staff and all types of information held by the organisation. This procedure should be read in conjunction with the organisation’s Information Governance (IG) policies.

## Chief Executive

This is the person with overall accountability/ responsibility for this policy and they and will work with the Executive team to ensure compliance with legislation.

## Caldicott Guardian

The Caldicott Guardian for the ICB is the Executive Director Clinical and Professional.

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate and secure information-sharing. The Guardian(s) plays a key role in ensuring that NHS, Councils with Social Services responsibilities, and partner organisations satisfy the highest practical standards for handling patient identifiable information. Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information.

* 1. **Senior Information Risk Owner (SIRO)**

The SIRO for the ICB is the Executive Director of Corporate Affairs.

The Senior Information Risk Owner (SIRO) will take overall ownership of the organisation’s information risks, act as champion for information risk on the Board and provide written advice to the Chief Executive on the content of the Organisation’s Annual Governance Statement in regard to information risk.

The SIRO must understand how the strategic business goals of the organisation and how other organisations business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the organisation and advises the Board on the effectiveness of information risk management across the organisation.

The SIRO is responsible for final approval of data protection impact assessments.

## Data Protection Officer (DPO)

The ICB’s Data Protection Officer is the Director of Governance and Board Secretary. The DPO will:

* + Monitor ICB compliance with the data protection responsibilities and obligations.
  + Provide advice and assistance with regards to the completion of Data Protection Impact Assessments
  + Act as a contact point for the Information Commissioners Office (ICO), members of the public and ICB staff on matters relating to data protection.
  + Assist in implementing essential elements of the data protection legislation such as the principles of data processing, data subjects’ rights, data protection impact assessments, records of processing activities, security of processing and notification and communication of data breaches.

## Senior Information Governance Manager

The Senior IG Manager supports the DPO and is responsible for the co-ordination of the implementation of systems within the ICB. The Senior IG Manager is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG across the ICB. The Senior IG Manager will:

* Support staff with the completion of DPIAs
* Suggest amendments to processes where necessary to ensure compliance with legislation.
* Provide advice and guidance to mitigate any data protection risks associated with the project.
* Raise any unmitigated risks with the SIRO, Risk Manager and if applicable the ICO.
* Ensure contracts and data sharing agreements are in place where necessary.
* Sign off DPIAs and make recommendations to the DPO and SIRO.

## Information Asset Owners & Administrators (IAOs & IAAs)

Information Asset Owners (IAO) are senior individuals involved in the running of their respective business functions and are directly accountable to the SIRO. IAOs must provide assurance that information risk is being managed effectively in respect of the information assets they are responsible for and that any new changes introduced to their business processes and systems undergo a data protection impact assessment where appropriate.

An Information Asset Administrator (IAA) will have delegated responsibility for the operational use of an Asset.

## Line Mangers

Managers are responsible for ensuring that their staff, both permanent and temporary, are aware of:

* + - The requirement to complete DPIAs and the requirements within all information security policies and guidance including their responsibility to comply with them.
    - Their personal responsibilities for information security
    - Where to access advice on matters relating to security and confidentiality; and
    - The security of their physical environments where information is processed or stored.

## All staff

All members of staff have a responsibility to ensure they are aware of all data protection, information security policies and guidance and comply with them. All staff leading on projects or procurement of systems and services must consider a data protection impact assessment. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use.

All staff are responsible for compliance with data protection legislation.

## Responsibilities for approval

The Senior Information Risk Owner under advisement of the Information Governance Steering Group is responsible for approving this policy.

# Consultation

All stakeholders such as ICB SIRO/DPO and Executive lead and IG leads involved in developing, implementing, managing, and monitoring data protection and confidentiality have been engaged in the development of this policy.

# Training

Staff with responsibility for completing DPIA’s will receive support as required from the Senior Information Governance Manager.

# Monitoring Compliance

Compliance will be monitored by the IG Team via completion and review of data protection impact assessments and review of the information asset register.

# Arrangements for Review

The policy will be reviewed every two years. Earlier review may be required in response to exceptional circumstances, organisational change, or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

# Dissemination

The policy will be disseminated by being made available on the ICB website and highlighted to staff through staff communications, and by managers.

# Associated Documentation

* Data Protection Impact Assessment Template – see appendix 3.
* Information Asset Owners Handbook
* Information Asset Register
* Dataflow Register
* Data Protection & Confidentiality Policy
* Information Governance Framework
* Records Management Policy
* National Data Opt-Out Policy

This list is not exhaustive.

# References

* Data Protection Act 2018
* General Data Protection Regulation (GDPR)
* Human Rights Act 1998 (Specifically Article 8)
* NHS England: NHS Standard Contract
* Information Commissioner: Data Sharing Code of Practice
* Information Commissioner: Data Protection Impact Assessments (DPIAs)

# Policy Document Requirements

## Why do I need to complete a DPIA?

HNY ICB staff must adhere to the requirements within this policy to demonstrate that privacy concerns have been considered and to assure HNY ICB regarding the security and confidentiality of personal information.

The DPIA template [(appendix 3)](#_Appendix_2_–) contains questions which cover all the Data Protection principles and prompt Project Managers/Leads to consider:

* whether all personal information is adequate relevant and necessary
* how the personal information will be kept up to date and checked for accuracy.
* whether personal identifiable information is required, or whether this could be pseudonymised.
* the legal basis for processing the personal information.
* transparency requirements, such as how individuals will be informed of the use of their information including rights such as rectification, restriction, objection, access,
* whether there is an audit function, to report who has accessed the information.
* how the personal information will be transferred.
* how/where the personal information will be stored.
* the security of the transfer, storage, and access to the information
* retention and destruction arrangements
* business continuity arrangement
* whether the personal information will be transferred outside the EEA

The DPIA procedure includes the requirement for review by the ICB’s Data Protection Officer and prior notification with the ICO, where applicable.

DPIAs identify privacy risks, foresee problems, and bring forward solutions.

A successful DPIA will:

* identify and manage risks in respect of privacy of personal information.
* avoid inadequate solutions to privacy risks.
* avoid unnecessary costs.
* avoid loss of trust and reputation
* inform the organisation’s communication strategy.
* meet or exceed legal requirements.

The Information Commissioners Office (ICO) has produced guidance materials on which this procedure is based: [Data Protection Impact Assessments (DPIAs) | ICO](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/)

DPIAs should demonstrate that privacy concerns have been considered and serve to assure the organisation regarding the security and confidentiality of the personal identifiable data.

## Is a DPIA required for every project?

Are you implementing a new system/data sharing arrangement/project or service, or changing the way you work?

Complete DPIA Screening Questions

No need to conduct a Data Protection Impact Assessment

Retain completed DPIA Screening Questions as part of project documentation.

Does this project involve the processing of personally identifiable or other high-risk data?

A Data Protection Impact Assessment is required.

Supporting information, such as contracts, system specifications and consent forms may be required (see Appendices)

Yes

Yes

No

No

*Figure 1*

No need to conduct a Data Protection Impact Assessment

DPIAs should be completed where a system/data sharing/project includes the use of personal data, where there is otherwise a risk to the privacy of the individual, utilisation of new or intrusive technology, or where private or sensitive data which was originally collected for a limited purpose will be reused in a new and ‘unexpected’ way.

## When Should I Start a DPIA?

DPIAs are most effective when they are started at an early stage of a project, when:

• the project is being designed

• you know what you want to do

• you know how you want to do it

• you know who else is involved

It must be completed before:

• decisions are set in stone

• you have procured systems/services

• you have signed contracts/Memorandum of Understanding/agreements

Following the review of the Screening Questions it should be determined whether or not a DPIA is required. Where it is thought that a DPIA is required, The DPIA Sections 1-4 should be completed and submitted to the Information Governance team for a preliminary review. Once reviewed the final DPIA will be submitted by the IG Team to the Data Protection Officer, and SIRO or Caldicott Guardian. Please note the controller is required under GDPR to contact the Information Commissioner’s Office if processing would result in a high risk in the absence of measures taken to mitigate the risk.

# Impact Assessments

## Equality

NHS Humber and North Yorkshire ICB is committed to creating an environment where everyone is treated equitably and the potential for discrimination is identified and mitigated. It aims to design and implement services, policies and measures that meet the diverse needs of our service, population, and workforce, ensuring that none are placed at a disadvantage over others.

An EQIA has been completed and as a result of performing the analysis the policy does not appear to have any adverse effects on people who share protected characteristics.

## Bribery Act 2010

Due consideration has been given to the Bribery Act 2010 in the development (or review, as appropriate) of this policy document, further details can be found in [appendix 2](#_Appendix_2_-).

## General Data Protection Regulations (GDPR)

The UK General Data Protection Regulation (GDPR)/ Data Protection Act 2018 includes the requirement to complete a Data Protection Impact Assessment for any processing that is likely to result in a high risk to individuals. Consideration should be given to any impact the policy may have on individual privacy; please consult NHS Humber and North Yorkshire ICB Data Protection Impact Assessment Policy. If you are commissioning a project or undertaking work that requires the processing of personal data, you must complete a Data Protection Impact Assessment.

The ICB is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and confidentiality guidance. More detailed information can be found in the Data Protection & Confidentiality Policy and related policies and procedures.

# Appendices

## Appendix 1 - The DPIA Procedure

At the start of any new project, commissioning of a new service, or implementation of a system, the Project Manager / Lead must complete the screening questions of the Data Protection Impact Assessment (DPIA), to ascertain whether the project will involve the new processing or any change in processing of Personal Confidential Data (PCD) and whether a full Data Protection Impact Assessment is required. This must also be completed when significant changes occur to an existing project, service, or system where it will affect or change the way in which personal confidential information is collected and processed.

If the answer to all the screening questions is NO, i.e., no PCD will be processed to develop and implement the project, service, or system, then this should be confirmed at the bottom of the Screening Questions. If required, the Information Asset Owner should be identified and a new Information Asset Risk Assessment and/or dataflow should be completed so that the Information Asset Register can be updated.

The screening questions must then be submitted to the Information Governance Specialist/ Information Governance Group to confirm the outcome is appropriate.

If the Answer is YES to any of the screening questions, or the review by the Information Governance Group requires it, then a full DPIA must be completed and submitted to the Senior Information Governance Manager to allow a full risk assessment of the use of personal confidential information within the project.

Completion of the full DPIA should identify the Information Asset Owner, who is then responsible for adding the projects information assets on to the ICB’s Information Asset Register, completing the Data Flow Map and checking whether there is an impact on the ICB’s Privacy Notice.

A report indicating potential risks and areas to be addressed will be prepared and returned to the project manager for agreed action. The Project Lead must complete the agreed action within the risk assessment and return it to the Senior Information Governance Manager for assessment of appropriateness of actions agreed.

Once appropriate action has been determined and recorded in the risk assessment report by the project lead, the original DPIA and the risk assessment report will be submitted to the ICB’s Data Protection Officer (DPO) for review.

If the DPO is satisfied all risks have been identified and appropriate mitigating action agreed to be implemented, then they will sign off the risk assessment and it will then go to the ICB SIRO or Caldicott Guardian for sign off.

If the DPO is not satisfied all risks have been appropriately addressed, then this will be raised with the ICB SIRO or Caldicott Guardian to prompt appropriate mitigating controls to be established and implemented. It should be noted that if significant risks are not appropriately mitigated then the DPO is duty bound to consult with the Information Commissioners Office.

The Project Manager/Lead, or identified Information Asset Owner, is responsible for keeping the DPIA under review until the project is completed. As projects can change throughout their implementation, it is important that all changes that affect the processing of personal information must be reported via the DPIA as they are identified to enable re-assessment of all processing of personal identifiable data. Any changes made to a DPIA must be reported to the Information Governance Team to provide the ICB with on-going assurance that the appropriate parts of the DPIAs have been completed for all projects and supports on-going monitoring.

The Senior Information Governance Manager will maintain a register of all new projects underway and due to commence, detailing the completion position of the DPIA to provide the ICB with on-going assurance that the appropriate parts of the DPIAs have been completed for all projects and supports on-going monitoring.

## Appendix 2 - Anti-Fraud, Bribery and Corruption

The ICB has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from the Bribery Act 2010. Under the Bribery Act 2010 there are four criminal offences:

* Bribing or offering to bribe another person (Section 1)
* Requesting, agreeing to receive or accepting a bribe (Section 2);
* Bribing, or offering to bribe, a foreign public official (Section 6);
* Failing to prevent bribery (Section 7).

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It should be noted that there need not be any actual giving and receiving for financial or other advantage to be gained, to commit an offence.

All individuals should be aware that in committing an act of bribery they may be subject to a penalty of up to 10 years imprisonment, an unlimited fine, or both. They may also expose the organisation to a conviction punishable with an unlimited fine because the organisation may be liable where a person associated with it commits an act of bribery.

Individuals should also be aware that a breach of this Act renders them liable to disciplinary action by the ICB, whether or not the breach leads to prosecution. Where a material breach is found to have occurred, the likely sanction will be loss of employment and pension rights.

To raise any suspicions of bribery and/or corruption please contact the Executive Director of Finance and Investment. Staff may also contact the Local Counter Fraud Specialist (LCFS) at – Audit Yorkshire, email: [nikki.cooper1@nhs.net](mailto:nikki.cooper1@nhs.net) or mobile 07872 988939.

The LCFS or Executive Director of Finance and Investment should be the contact for any suspicions of fraud. The LCFS will inform the Executive Director of Finance and Investment if the suspicion seems well founded and will conduct a thorough investigation. Concerns may also be discussed with the Executive Director of Finance and Investment or the Audit Committee Chair.

If staff prefer, they may call the NHS Counter Fraud reporting line on 0800 028 40 60 between 8am-6pm Monday-Friday or report online at www.reportnhsfraud.nhs.uk. This would be the suggested contact if there is a concern that the LCFS or the Executive Director of Finance and Investment themselves may be implicated in suspected fraud, bribery or corruption.

## Appendix 3 – DPIA Template

**Data Protection Impact Assessment (DPIA) Screening Questions**

The below screening questions should be used to inform whether a DPIA is necessary. This is not an exhaustive list therefore in the event of uncertainty, completion of a DPIA is recommended. If you are unsure or need any support completing this document, please contact the IG Team at:

[hnyicb-ery.ig@nhs.net](mailto:hnyicb-ery.ig@nhs.net)

|  |  |
| --- | --- |
| **Title** |  |
| **Brief description**  Please provide a brief overview explaining the project/ system/ service. |  |

*Screening completed by*

|  |  |
| --- | --- |
| **Name** |  |
| **Title** |  |
| **Department** |  |
| **Email** |  |
| **Date** |  |

Marking any of these questions is an indication that a DPIA is required:

|  |  |  |
| --- | --- | --- |
| **Screening Questions** | | **Tick** |
| 1 | Will the project involve the collection of new identifiable or potentially identifiable (pseudonymised) data about individuals?  (If the ICB do not process personal data but another organisation or a service provider does as part of the project, a DPIA must still be completed). |  |
| 2 | Will the project compel individuals to provide data about themselves or involve the processing of personal data not obtained directly from the individual?  i.e., where they will have little awareness or choice or where it is impossible, or would involve disproportionate effort, to inform the individuals that the processing is taking place |  |
| 3 | Will identifiable data about individuals be shared with other organisations or people who have not previously had routine access to the data? |  |
| 4 | Are you using data about individuals for a purpose it is not currently used for or in a new way?  i.e., using data collected to provide care for a service evaluation; data matching where data obtained from multiple sources is combined, compared or matched. |  |
| 5 | Where data about individuals is being used, would this be likely to raise privacy concerns or expectations?  i.e., will it include health records, genetic data, criminal records or other information that people may consider to be sensitive and private and may cause them concern or distress. |  |
| 6 | Will the project require you to contact individuals in ways which they may find intrusive?  i.e., telephoning or emailing them without their prior consent. |  |
| 7 | Will the project result in you making decisions in ways which can have a significant impact on individuals?  i.e., will it affect the care a person receives? Is it based on automated decision making (including profiling)? |  |
| 8 | Does the project involve you using new technology which might be perceived as being privacy intrusive?  i.e., using biometrics, facial recognition, Artificial Intelligence or tracking (such as tracking an individual’s geolocation or behaviour) |  |
| 9. | Is a service/processing activity being transferred to a new supplier/organisation (or re-contracted) at the end of an existing contract |  |
| 10. | Will the project involve systematic monitoring of a publicly accessible area on a large scale?  i.e., use of CCTV |  |
| 11. | Will the project involve the targeting of children or other vulnerable individuals?  i.e. for marketing purposes, profiling or other automated decision making |  |
|  |  |  |
| \* | If none of the above are applicable, please tick to confirm you have considered completion of a DPIA and determined it is not required. |  |

*Please retain a copy of this questionnaire within your project/system documentation.*

**Data Protection Impact Assessment (DPIA)**

Please complete all questions with as much detail as possible (liaising with partners/third parties) and then contact the IG Team prior to seeking approval.

**Section 1: System/Project General Details**

|  |  |  |
| --- | --- | --- |
| **System/project/process (referred to thereafter as ‘project’) title:** |  | |
| **Objective:** Please explain your objectives, what are you trying to achieve? |  | |
| **Detail:** Why is the new system/change in system required? Is there an approved business case? |  | |
| **Stakeholders/Relationships/Partners:** Please outline the nature of such relationships and the corresponding roles of other organisations. |  | |
| **Data Controller:**  The controller is the organisation that alone or jointly determines the purpose and means of the processing. Eg. ICB, GP, Trust, Local Authority  [What are ‘controllers’ and ‘processors’? | ICO](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/) | Name the Data Controllers / Joint Data Controllers (Please list all): | |
| **Other related projects:** |  | |
| **Project lead:** | Name: |  |
| Title: |  |
| Department: |  |
| Telephone: |  |
| Email |  |
| **Information Asset Owner:**  All information systems/assets must have an [Information Asset Owner (IAO).](file:///C:\Users\melissa.willis\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\01HVOVOV\DPIA%20V9%20DRAFT%20Template%2001.12.23.docx#IAO) IAO’s should normally be a Head of Department/Service. | Name: |  |
| Title: |  |
| Department: |  |
| Telephone: |  |
| Email |  |
| **Information Asset Administrator:**  Information systems/assets may have an [Information Asset Administrator (IAA)](file:///C:\Users\melissa.willis\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\01HVOVOV\DPIA%20V9%20DRAFT%20Template%2001.12.23.docx#IAA) who reports the IAO. IAA’s are normally System Managers/Project Leads. | Name: |  |
| Title: |  |
| Department: |  |
| Telephone: |  |
| Email |  |

**Section 2: Data Protection Impact Assessment Key Questions**

|  | **Question** | **Response** |
| --- | --- | --- |
| **Data Items** | | |
|  | **Will the project use identifiable or potentially identifiable data in any way?**  If answered ‘No’ then a DPIA is not normally suggested. | Yes  No  If yes, who will this data relate to:  Patient  Staff  Other: Click here to enter text. |
|  | **Please state purpose for the processing of the data:**  For example, patient care, commissioning, research, audit, evaluation. |  |
|  | **Will the processing be ongoing or for a fixed term?** | Ongoing  Fixed Term  If fixed term please explain: |
|  | **Please tick the data items that are held in the system**  **Personal**    **Special categories**  **of personal data**  **(sensitive data)** | Name  Address  Post Code  Date of Birth  GP Practice  Date of Death  NHS Number  NI Number  Passport Number  Pseudonymised Data  Online Identifiers (e.g. IP Number, Mobile Device ID)  Health Data  Trade Union membership  Political opinions  Religion  Racial or Ethnic Origin  Sex life and sexual orientation  Biometric Data  Genetic Data    Other: |
|  | **What consultation/checks have been made regarding the adequacy, relevance and necessity for the processing of the data for this project?**  (For example - why do you need all the data items in section 3, why can’t you achieve the intended purpose with less data, anonymised data etc.) |  |
|  | **How will the data be kept up to date and checked for accuracy and completeness?** |  |
|  | **What is the scope of the processing?** | **Data Subject(s):**  <100  100 – 500  501 – 1,000  1,001 – 10,000  10,001 – 50,000  >50,000  Unknown  **Records:**  <100  100 – 500  501 – 1,000  1,001 – 10,000  10,001 – 50,000  >50,000  Unknown |
| **Data processing** | | |
|  | **Will a third party be processing data on behalf of the ICB or one of its contractors?** | Yes  No  If no, please go to the Confidentiality section. |
|  | **Name and address of the third party:** |  |
|  | **Is the third party contract/supplier of the project registered with the Information Commissioner?** | Yes  No  Organisation:  Data Protection Registration Number: |
|  | **Has the third party supplier completed and published a satisfactory** [**Data Security and Protection Toolkit submission**](https://www.dsptoolkit.nhs.uk/)**?** | Yes  No  If yes, please give organisation code:  **DSPT Toolkit score:**  Standards Met  Approaching Standards  Standards Exceeded  Improvement Plan Submitted  Not applicable – no patient data processed |
|  | **Does the third party/supplier contract(s) include all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?** | Yes  No  Is the contract based on or utilise the NHS standard contract?  Yes  No  Is the Contract a Crown Commercial Services contract?  Yes  No |
|  | **Will the third party sub-contract any work in relation to this processing?** | Yes  No  If yes please list the subcontractors and their purpose: |
|  | **Will other third parties (not already identified) have access to the data?** Include any external organisations. | Yes  No  If so, for what purpose?  Please list organisations and by what means of transfer: |
| **Confidentiality** | | |
|  | **Please outline how individuals will be informed and kept informed about how their data will be processed.**  A copy of the [privacy notice and/or leaflets](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) must be provided. |  |
|  | **Does the project involve the collection of data that may be unclear or intrusive?** Are all data items clearly defined? Is the data collected limited to a specific set of predefined categories? | Yes  No  If yes, please explain: |
|  | **Are you relying on individuals (patients/staff) to consent to the sharing of personal identifiable or sensitive data?**  Please provide copies of any consent documentation that will be used, including patient information leaflets | Yes  No (Go to next question)  How will consent be obtained and by whom?  Click here to enter text.  Will the consent cover all proposed sharing/disclosures?  Yes  No  If no, please detail:  Click here to enter text. |
|  | **What legal basis enables this data processing?**  For more information about conditions for processing, please see the [ICO’s GDPR website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/). | Personal data (identifiers and potentially identifiable data):  Relating to a contract: Click here to enter text.  Legal obligation: Click here to enter text.  Vital interests: Click here to enter text.  Public task: Click here to enter text.  Other: Click here to enter text.  Special categories of personal data (sensitive data), *if applicable*:  Medical related: Click here to enter text.  Public Health: Click here to enter text.  Employment related: Click here to enter text.  Vital interests: Click here to enter text.  Already public: Click here to enter text.  Legal claim related: Click here to enter text.  Substantial public interest: Click here to enter text.  Other: Click here to enter text. |
|  | **Will identifiable data only be handled within the patients’ direct care team (in accordance with the** [**Common Law Duty of Confidentiality**](file:///C:\Users\melissa.willis\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\01HVOVOV\DPIA%20V9%20DRAFT%20Template%2001.12.23.docx#CommonLaw)**)?** | Yes  No  If no, please detail: |
|  | **How will consent, non-consent, objections or opt-outs be recorded and respected?** |  |
|  | **What arrangements are in place to process Subject Access Requests?** What would happen if such a request were made? |  |
|  | **Will the processing of data be automated?** Will the proposed processing of data involved automated means of processing to determine an outcome for the individual? | Yes  No  Not applicable  If yes, please outline what arrangements are available to enable the individual access and to extract data (in a standard file format). Please also detail any profiling that may take place as part through automated processing:  Click here to enter text. |
|  | **What process is in place for rectifying/blocking data?** What would happen if such a request were made? |  |
| **Engagement** | | |
|  | **Has stakeholder engagement taken place?** | Yes  No  If yes, how have any issues identified by stakeholders been considered?  Click here to enter text.  If no, please outline any plans in the near future to seek stakeholder feedback:  Click here to enter text. |
| **Data Sharing** | | |
|  | **Does the project involve any new data sharing between stakeholder organisations?** | Yes  No  If yes, please describe:  Click here to enter text.  Please provide a high level data flow diagram showing how identifiable information would flow.  Yes  No |
|  | **Is this use or disclosure of data in scope for the national data opt- out to be applied?**  **(Data used for research or planning is in scope)** [National data opt-out - NHS Digital](https://digital.nhs.uk/services/national-data-opt-out)  ***(Please see the ICB’s NDOO Policy at:*** [Documents and Publications (icb.nhs.uk)](https://humberandnorthyorkshire.icb.nhs.uk/documents-and-publications/) or ***contact your IG lead if you need more information about this)*** | Yes  No  If yes please explain how this will be managed, and how patients can opt- out: |
| **Data Linkage** | | |
|  | **Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?**  The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a collection of a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously) | Yes  No  If yes, please provide a data flow diagram showing how identifiable information would flow and ensure this is added to the ICB Information Asset and Data Flow Register (see Information Assets and Data Flows section). |
| **Information Security** | | |
|  | **Who will have access to the data within the project?**  Please refer to roles/job titles/organisations. | Click here to enter text. |
|  | **Is there a useable audit trail in place for the project?**  For example, to identify who has accessed a record? | Yes  No  Not applicable  If yes, please outline the audit plan: Click here to enter text. |
|  | **Where will the data be kept/stored/accessed?**  Where applicable, please refer to data flow diagram. | Click here to enter text. |
|  | **Has the organisation responsible for the storage of data implemented port controls? Eg. are USB ports, CD writers etc. disabled or restricted?** |  |
|  | **Please indicate all methods in which data will be transferred** | Fax  Email (Unsecure/Personal)  Email (Secure/nhs.net)  Internet (unsecure – e.g. http)  Telephone  Internet (secure – e.g. https)  By hand  Courier  Post – track/traceable  Post – normal  Software  Mobile app  Other: Click here to enter text. |
|  | **Does the project involve privacy enhancing technologies?**  *New forms* of encryption, two factor authentication and/or pseudonymisation. | Yes  No  If yes, please give details: Click here to enter text. |
|  | **Is there a documented System Level Security Policy (SLSP) or process for this project?**  A [SLSP](file:///C:\Users\melissa.willis\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\01HVOVOV\DPIA%20V9%20DRAFT%20Template%2001.12.23.docx#SupportingDocs) is required for new *systems* – this is likely to need to be completed by the supplier. | Yes  No  Not applicable  If yes, please provide a copy. |
| **Privacy and Electronic Communications Regulations** | | |
|  | **Will the project involve the sending of unsolicited marketing messages electronically such as telephone, fax, email and text?**  [Please note that seeking to influence an individual is considered to be marketing.](file:///C:\Users\melissa.willis\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\01HVOVOV\DPIA%20V9%20DRAFT%20Template%2001.12.23.docx#PECR) | Yes  No  If yes, what communications will be sent?  Click here to enter text.  Will consent be sought prior to this?  Yes  No  If no, please explain why consent is not being sought first:  Click here to enter text. |
| **Records Management** | | |
|  | **What are the specific retention periods for this data?**  Please refer to the [Records Management Code of Practice for Health and Social Care 2016](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/records-management-code-of-practice-for-health-and-social-care-2016) and list the retention period for identifiable project datasets. | Click here to enter text. |
|  | **Will the data be securely destroyed when it is no longer required?** | Yes  No  If no, please detail: Click here to enter text. |
| **Information Assets and Data Flows** | | |
|  | **Has an** [**Information Asset Owner**](file:///C:\Users\melissa.willis\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\01HVOVOV\DPIA%20V9%20DRAFT%20Template%2001.12.23.docx#IAO) **been identified and does the** [**Information Asset**](file:///C:\Users\melissa.willis\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\01HVOVOV\DPIA%20V9%20DRAFT%20Template%2001.12.23.docx#InfoAssets) **and Data Flow Register require updating?**  Please see the [Information Asset Register and Data Flow Mapping Form](file:///C:\Users\melissa.willis\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\01HVOVOV\DPIA%20V9%20DRAFT%20Template%2001.12.23.docx#SupportingDocs). | Yes  No  If yes, include the completed Information Asset Register New Entry Form.  Does this project constitute a change to existing Information Asset(s) or is this a new Information Asset?  Yes  No  If yes, include the completed Information Asset Register and Data Flow Mapping Form for risk review. |
| **Business Continuity** | | |
|  | **Have the business continuity requirements been considered?** | Yes  No  Business Continuity is not applicable  Please explain and either reference how such plans link with the organisational plan or why there are no business continuity considerations that are applicable for this project: Click here to enter text. |
| **Open Data** | | |
|  | **Will identifiable/potentially identifiable from the project be released as Open Data (placed in to the public domain)?** | Yes  No  If yes, please describe: Click here to enter text. |
| **Data Processing Outside of the UK and European Union (EU)** | | |
|  | **Will any personal and/or sensitive data be transferred to a country outside the UK?** | Yes  No  If yes, which data and to which country?  Click here to enter text. |
| **Artificial Intelligence (AI) \*If you are not using AI you do not need to complete this section\*** | | |
|  | **Does the project involve the use of Artificial intelligence (AI)**  You must read the ICB’s Artificial Intelligence Policy if you are completing this section. | Yes  No  If you have answered no you do not need to complete this section. |
|  | **Please explain in detail how you intend to use AI.** |  |
|  | **Please provide information on how the AI output is used to make decisions and the potential impact on data subjects, including any potential negative impacts.** |  |
|  | **Please explain the logic behind the decision making in a clear and simple way.** |  |
|  | **When an output is produced is there a human to review this outcome or is the final decision making solely reliant on AI?** |  |
|  | **How will you be recording the AI informed decision making with regards to the data subject? (Patient care/staffing decision etc.)** |  |
|  | **Have you consulted with individuals that are likely to be affected by the use of AI?** |  |
|  | **What sources of data were used to originally train the algorithm? How was this chosen? How was this validated and data quality issues worked out?** |  |
|  | **Please provide a data flow diagram.** |  |
|  | **How does the product avoid discrimination between different groups? How has bias been mitigated?** |  |
|  | **What training will be done with staff members so they can interpret outputs of the AI decision making effectively?** |  |
|  | **What accuracy rates and other performance metrics have you chosen for the model and how was this agreed?** |  |
|  | **Will the person who is required to use the output be shown the decision metrics and decision pathways before being required to make a decision?** |  |
|  | **What mechanism is there for flagging any consistent issue with outputs generated by this product?** |  |
|  | [**If this is a health technology has a DTAC been completed? Does this include Hazard log and clinical safety case (ensure this is submitted to the CSO)**](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftransform.england.nhs.uk%2Fkey-tools-and-info%2Fdigital-technology-assessment-criteria-dtac%2F&data=05%7C01%7Chayley.gillingwater%40nhs.net%7Cd0bf3995c1f54124800908db7e3f907a%7C37c354b285b047f5b22207b48d774ee3%7C0%7C0%7C638242583684247379%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=9VyU%2BO5ZOTnRenqmCnqZKN%2BDSmyrfptDcI0JDIRcL%2F8%3D&reserved=0) |  |
|  | [**Is this classed as a medical device as defined by the MHRA?**](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.gov.uk%2Fgovernment%2Fpublications%2Freport-a-non-compliant-medical-device-enforcement-process&data=05%7C01%7Chayley.gillingwater%40nhs.net%7Cd0bf3995c1f54124800908db7e3f907a%7C37c354b285b047f5b22207b48d774ee3%7C0%7C0%7C638242583684247379%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=UUuD12qaVmZclLnVNxxTwUfY0%2BJC6pJjKCS4JqAjP9M%3D&reserved=0) |  |
|  | **How will the AI algorithm develop over time? Will personal data be required to train the AI? If yes, what data would be required?** |  |
|  | **Are there plans in place for ongoing review of the product? How often does this happen? How is information from the review fed back and to whom?** |  |
|  | **What is the escalation route if an output needs to be disputed? Who will lead this?** |  |
|  | **Has the implementation of AI been discussed with the IT department?** |  |

**Section 3: Data Protection Impact Assessment Information Governance Review**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Information Governance Review (for completion by IG)** | | | | **Response (for completion by project lead)** | |
| **Issue** | | **Potential Risk** | **Recommendation** | **Agreed Action** | **Completion (Date and Initials)** |
| **1** |  |  |  |  |  |
| **2** |  |  |  |  |  |
| **3** |  |  |  |  |  |
| **4** |  |  |  |  |  |
| **5** |  |  |  |  |  |

*For completion by IG:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Residual Risk** | | **Initial Risk Score** | **Main Controls Reducing the Severity and Likelihood** | **Severity** | **Likelihood** |
| **1** |  |  |  |  |  |
| **2** |  |  |  |  |  |
| **3** |  |  |  |  |  |

**IG review completed by:**  Click here to enter text. **Review date:**  Click here to enter text.

**Date complete and risk assessed:** Click here to enter text. **Consultation with ICO required? Yes/No (delete as appropriate)**

**Section 4: Review and Approval**

**Assessment completed by**

|  |  |
| --- | --- |
| **Name:** | Click here to enter text. |
| **Title:** | Click here to enter text. |
| **Date:** | Click here to enter text. |

**Data Protection Officer Approval**

|  |  |
| --- | --- |
| **Name:** |  |
| **Title:** |  |
| **DPO advice:**  DPO should advise on compliance, risks identified and whether processing can proceed.  If accepting any residual high risk, consult the ICO before going ahead |  |
| **Approved** |  |
| **Date:** |  |

The DPO should also review ongoing compliance with DPIA

**SIRO/Caldicott Guardian Approval**

|  |  |
| --- | --- |
| **Name:** |  |
| **Title:** |  |
| **DPO advice accepted or overruled:**  If overruled, you must explain your reasons |  |
| **Approved:** |  |
| **Date:** |  |