## 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).](#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)](#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**](#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](#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.](#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**](#IAO) **been identified and does the** [**Information Asset**](#InfoAssets) **and Data Flow Register require updating?**  Please see the [Information Asset Register and Data Flow Mapping Form](#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:** |  |