**appendix 4 – DBTH data prOTECTION impact assessment (dpia)**

****

**Appendix 4 to CORP/ICT 3**

**DBTH Data Protection Impact Assessment (DPIA)**

**Project/Information Asset Title:**

|  |
| --- |
| **DPIA Initiation and Review** |
| **Privacy Marking** | **Unrestricted** |
| Author/reviewer:  |  |
| Information Asset Owner (IAO) |  |
| Project Manager (PM) - when applicable |  |
| Date written/revised: |  |
| Approved by: | Information Governance Committee |
| Date of approval: |  |
| Target audience: | Trust wide |
| **Version Control Log** |
| **Version**  | **Name** | **Date** |
| V1 |  |  |
|  |  |  |
|  |  |  |

**Steps 1 to 5:** are intended to help you as the IAO and/or the PM to decide whether a DPIA is necessary, and to then provide as much detail as possible. Don’t worry, the Information Governance Committee are there to help.

**For the avoidance of doubt in this DPIA:** An **asset** is a registered database system or on-line application that is used to process personal information. See [Trust Policy CORP/ICT 3](https://www.dbth.nhs.uk/about-us/our-publications/publication-scheme/our-policies-and-procedures/policies-a-to-z/) for clarification, or get advice from: dbth.dpo@nhs.net

**Answering ‘yes’ to any of the questions below is an indication that a DPIA would be appropriate.** You can expand on your answers as the project develops if you need to.

# Step 1: Initial questions for the Information Asset Owner and the Project Team

|  |
| --- |
| **Y N** |
| Will the project/asset involve the collection of individuals personal information? | [ ]  | [ ]  |
| Will the project/asset compel individuals to provide personal information about themselves? | [ ]  | [ ]  |
| Will personal information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | [ ]  | [ ]  |
| Are you using personal information about individuals for a purpose it is not currently used for, or in a way it is not currently used? | [ ]  | [ ]  |
| Does the project/asset involve the use of new technology that might be perceived as being privacy intrusive? | [ ]  | [ ]  |
| Will the project/asset result in you making decisions or taking action against individuals in ways that could have a significant/adverse impact on them? | [ ]  | [ ]  |
| Is the personal information about individuals of a kind that is likely to raise privacy concerns or expectations? For example, health records, criminal records, or other personal information that people consider to be private. | [ ]  | [ ]  |
| Will the asset require you to contact individuals in ways that they may find intrusive? | [ ]  | [ ]  |
| Looking at where you have indicated a Y (Yes), it is now necessary that a full DPIA review is appropriate. Please tell us ‘briefly’ the purpose below, and then move on to section 2, unless you need further guidance from: dbth.dpo@nhs.net  |
| If personal data are going to be processed, **what is the purpose** of that processing?For example, patient care, commissioning, research, clinical audit, or information evaluation that includes a personal data element |  |

#

# Step 2. Data Protection Impact Assessment template

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale DPIAs might record this information on the more formal Corporate DATIX System Risk Register.

|  |  |  |  |
| --- | --- | --- | --- |
| **Threats****(Risks)** | **Controls** | **Likelihood x Consequence** **= Impact** (5 x 5 = 25) | **Corporate Risk** **>15**(Y or N) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Step 3: Data Protection Impact Assessment - Key Questions**

|  |
| --- |
| **Information Governance Questions** |
|  | **Will the system/project/process (referred to thereafter as ‘project’) contain identifiable or Personal Confidential Data (PCD)?** | [ ]  Yes [ ]  NoIf yes, who will this data relate to:[ ]  Patient[ ]  Staff[ ]  Other: If answered ‘No’ then **a DPIA is not required** however, where the project would benefit from completion then the DPIA will help to catalogue and to mitigate any risks to trust information assets |
|  | **Please tick the personal data items that are held in the system****Demographic****Data****Special** **Category** **Data****Completing the Date of Death indicates that the personal data record is not covered by the DPA 2018 or the UK GDPR** |  [ ]  Name [ ]  Address [ ]  Post Code [ ]  Date of Birth [ ]  GP Practice [ ]  Date of Death [ ]  NHS Number [ ]  NI Number[ ]  Medical History [ ]  Trade Union membership[ ]  Political opinions [ ]  Religion[ ]  Ethnic Origin [ ]  Sexuality[ ]  Criminal offences [ ]  Other:  |
|  | **What consultation/checks have been made regarding the adequacy, relevance and necessity for the collection of personal and/or sensitive data for this project?** | Click here to enter text. |
|  | **How will the information be kept up to date and checked for accuracy and completeness?** | Click here to enter text. |
| **Information Assets and Data Flows** |
|  | **Has an Information Asset Owner been identified and does the Information Asset Register require updating?** | [ ]  Yes [ ]  NoIf yes, include a complete Information Asset Register entry as per [Trust Policy CORP/ICT 3](http://dbhdatixweb/datix/live/index.php?action=record&module=COM&recordid=12393). |
|  | **Have the data flows been captured?** | [ ] Yes [ ] NoIf yes, include in the completed Information Asset Register entry (see 5 above). |

|  |
| --- |
| **Data processing** |
|  | **Will a third party be processing data?** | [ ]  Yes [ ]  No[ ]  Not applicableIf No, please go to the Confidentiality section.  |
|  | **Is the third party contract/supplier of the project registered with the Information Commissioner?** [SEARCH REGISTER](https://ico.org.uk/esdwebpages/search) | [ ]  Yes [ ]  No[ ]  Not applicableOrganisation: Click here to enter text.Data Protection Registration Number: Click here to enter text. |
|  | **Has the third party supplier completed a Data Security and Protection Toolkit Return?** | [ ]  Yes [ ]  No[ ]  Not applicableIf yes, please state level of Standard Met. |
|  | **Does the third party/supplier contract(s) contain all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?** | [ ]  Yes [ ]  No[ ]  Not applicable*If the contract has been let under the NHS Standard Terms & Conditions for the Supply of Services then tick* ***Yes*** |
|  | **Will other third parties (not already identified) have access to the project?** Include any external organisations. | [ ]  Yes [ ]  No[ ]  Not applicableIf so, for what purpose?Click here to enter text.Please list organisations and by what means of transfer – Data Flows:Click here to enter text. |
| **Confidentiality** |
|  | **Please outline what Privacy Notices (PNs) and associated leaflets – if any - will be provided.**Please provide copy of or links to any none DBTH PNs etc.[DBTH PN’s can be found here](https://www.dbth.nhs.uk/about-us/our-publications/information-governance/control-patient-information-notice-covid-19-outbreak/) | Click here to enter text. |
|  | **Does the project involve the collection of data that may be unclear or intrusive?**Are all data items clearly defined? Is there a wide range of sensitive data being included? | [ ]  Yes [ ]  No[ ]  Not applicable |
|  | **Are you relying on individuals (patients/staff) to consent to the processing of personal identifiable or sensitive data?**  | [ ]  Yes [ ]  No[ ]  Not applicableIf yes, what type of consent will be sought?[ ]  Explicit [ ]  ImplicitHow will that consent be obtained and by whom?Click here to enter text.If No, which GDPR legal basis/justification is being used instead, such as:[ ]  Medical purpose 9 2(h) [ ]  Public Interest 6 1(e)[ ]  Court Order [ ]  Other: Click here to enter text. |
|  | **How will consent, non-consent, objections or opt-outs be recorded and respected?** | Click here to enter text. |
|  | **Will the consent cover all processing and sharing/disclosures?**  | [ ]  Yes [ ]  No[ ]  Not applicableIf not, please detail: Click here to enter text. |
|  | **What process is in place for rectifying/blocking data?**What would happen if such a request were made? |  Click here to enter text. |
| **Engagement** |
|  | **Has stakeholder engagement taken place?** | [ ]  Yes [ ]  No[ ]  Not applicableIf 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 information sharing between organisations?**  | [ ]  Yes [ ]  No[ ]  Not applicableIf yes, please describe:Click here to enter text.**Please provide a concise data flow listing and/or a diagram if you have one.** |

|  |
| --- |
| **Data Linkage** |
|  | **Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?** | [ ]  Yes [ ]  No[ ]  Not applicableIf yes, **Please provide a concise data flow listing and/or a diagram if you have one.**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) |
| **Business Continuity** |
|  | **Have the requirements for business continuity been considered?** | [ ]  Yes [ ]  No[ ]  Not applicableIf yes, please detail: Click here to enter text. |
| **Records Management** |
|  | **What are the retention periods for this data?** Please refer to the [Records Management: NHS Code of Practice](http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf). | Click here to enter text. |
|  | **How will the data be destroyed when it is no longer required?** | Click here to enter text. |
| **Open Data** |
|  | **Will (potentially) identifiable and/or sensitive information from the project be released as Open Data (be placed in to the public domain)?** | [ ]  Yes [ ]  No[ ]  Not applicableIf yes, please describe: Click here to enter text. |
| **Data Processing Outside of the UK**  |
|  | **Will (potentially) identifiable and/or sensitive information from the project be released outside of the UK**  | [ ]  Yes [ ]  No[ ]  Not applicableIf yes, please describe: Click here to enter text. |

|  |
| --- |
| **Data/IT Security Questions** |
|  | **Who will have access to the information within the system?**Please refer to roles/job titles. | 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 applicableIf yes, please outline the audit plan: Click here to enter text. |
|  | **Describe where will the information be kept/stored/accessed?** | Click here to enter text. |
|  | **Please indicate all methods in which information will be transferred** | [ ]  Fax [ ]  Email (Unsecure/Personal)[ ]  Email (Secure/nhs.net) [ ]  Internet (unsecure – eg. http)[ ]  Telephone [ ]  Internet (secure – eg. https)[ ]  By hand [ ]  Courier[ ]  Post – track/traceable [ ]  Post – normal[ ]  Other: Click here to enter text. |
|  | **Does the project involve privacy enhancing technologies?**Encryption; 2 factor authentication, new forms of Pseudonymisation. | [ ]  Yes [ ]  No[ ]  Not applicableIf 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 is required for new systems. | [ ]  Yes [ ]  No[ ]  Not applicableIf 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. | [ ]  Yes [ ]  No[ ]  Not applicableIf yes, what communications will be sent?Click here to enter text.Will consent be sought prior to this?[ ]  Yes [ ]  No[ ]  Not applicable |

**The IAO is:**

* responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork
* responsible for implementing the solutions that have been approved
* the contact for any privacy concerns that may arise in the future

**Step 4: Integrate the DPIA outcomes back into the project plans where necessary**

|  |  |  |
| --- | --- | --- |
| Action to be taken | Date for completion of actions | Responsibility for action |
|  |  |  |

|  |
| --- |
| Contact point for future privacy concerns with this DPIA: |

**Step 5: Review and Approval**

**Assessment completed by**

|  |  |
| --- | --- |
| **Name:** | Click here to enter text. |
| **Title:** | Click here to enter text. |
| **Sent electronically or Signed:** |[ ]
| **Date:** | Click here to enter text. |

**Assessment reviewed (IG) by**

|  |  |
| --- | --- |
| **Name:** | Click here to enter text. |
| **Title:** | Click here to enter text. |
| **Reviewed electronically or Signed:** |[ ]
| **Date:** | Click here to enter text. |

**Assessment reviewed (IT Ops) by**

|  |  |
| --- | --- |
| **Name:** | Click here to enter text. |
| **Title:** | Click here to enter text. |
| **Reviewed electronically or Signed:** |[ ]
| **Date:** | Click here to enter text. |

**Data Protection Officer Approval**

|  |  |
| --- | --- |
| **Name:** | Click here to enter text. |
| **Title:** | Click here to enter text. |
| **Reviewed electronically or Signed:** |[ ]
| **Any additional comments** |  |
| **Date:** | Click here to enter text. |

**Information Governance Committee (IGC) Approval and any instructions from the SIRO or Caldicott Guardian**

|  |  |
| --- | --- |
| **IGC Chair:** | Click here to enter text. |
| **Title:** | Click here to enter text. |
| **Any additional comments from SIRO or CG** |  |
| **IG Committee Date:** | Click here to enter text. |