**Data Protection Impact Assessment**

**Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Reference No: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (IG Use only)**

A Data Protection Impact Assessment (DPIA) is required for any new process or project in order to assess compliance with the General Data Protection Regulation / Data Protection Act 2018 and to help manage any risks to individual’s privacy. The document also demonstrates that risks have been considered and appropriate measures have been taken to comply with the legislation. The Trust can be fined if we fail to carry out a DPIA for certain types of processing, or if we carry it out incorrectly.

Information Governance can assist you with this process and will complete sections of the document to assess their view of the systems or projects compliance.

Please complete sections 1 and 2 (and section 3 if the project includes a new ICT system or function) then send the document to Information Governance [rdash.ig@nhs.net](mailto:rdash.ig@nhs.net)

IG will complete sections 4 and 5 and contact you for any further information required.

When all queries have been resolved the DPIA will need to be signed off by:

* Project Manager or Service Manager (originator of DPIA)
* Information Asset Owner (normally Head of Service)
* Director of the Service
* Information Governance
* Data Protection Officer (DPO)
* IT Specialist (as necessary)

Wherever possible DPIAs should be published and made available to the public. There are some exceptions to this or we may redact some details and publish the document. This will form part of IG’s assessment at Section 6.

Some DPIAs will need approval from the Information Commissioner’s Office. Information Governance/ the DPO will analyse whether this is required and notify you accordingly during the process.

**Screening questions**

**To be completed by the Service Area -** These questions will determine whether a DPIA is necessary. If the answer is ‘yes’ to any of the following questions you will need to complete the full DPIA.

|  |  |  |
| --- | --- | --- |
|  | Will the project involve the collection or use of personal information? |  |
|  | Will the project compel individuals to provide information about themselves? |  |
|  | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information (including RDaSH colleagues? |  |
|  | Are you using information about individuals for a purpose it is not currently used for or in a way it is not currently used? |  |
|  | Does the project involve you using new technology which might be perceived as being particularly privacy intrusive? E.g. Use of biometrics or facial recognition? |  |
|  | Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? |  |
|  | Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? E.g. Health records, criminal records or other information that people would consider particularly private? |  |
|  | Will the project require you to contact individuals in ways which they may find particularly intrusive? |  |
|  | Does the project involve processing large volumes of personal data or data about a large number of individuals? |  |
|  | Does the system have a cost? |  |
|  | Does the system have an approved budget? |  |
|  | Is a contract required for the system?  If, Yes please ensure the due diligence questionnaire is completed and returned. |  |

**Section 1 - Project Details**

|  |  |  |
| --- | --- | --- |
| Project name/ title: |  | |
| Originator/Project Manager | Name |  |
| Title |  |
| Dept. & Team |  |
| Telephone |  |
| Information Asset Owner | Name |  |
| Title |  |
| Dept. & Team |  |
| Telephone |  |
| Director Approval  **Director Approval is required for systems or processes that incur a cost, require an approved budget or require approval for clinical use.** | Name |  |
| Title |  |
| Dept. & Team |  |
| Telephone |  |
| Describe the project or new system |  | |
| Why is this change required and what benefits will it bring? |  | |
| Please describe the flow of the information, a flow diagram may be of assistance |  | |

**NOTE: Completion and sign off of a DPIA or systems installation process by the Information Governance (IG) or Information Technology (IT) departments, does not indicate approval of software applications on behalf of the organisation that provide clinical information, nor confirm the accuracy of clinical information contained within them.**

**Section 2 – Privacy Impact Questions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Who to Complete?** | **Question** | **Response** | **Guidance** |
| Service Area | 1. Who is the Data Controller for the information you are using?  Are there any other data controllers or data processors involved in the project/change? |  | * A data controller is the organisation that determines the purposes and means of processing personal data. * A processor is responsible for processing personal data on behalf of a controller. |
| Service Area | 2. Please state why you are collecting or using information. |  |  |
| Service Area | 3. Who will you be collecting information about? |  | e.g. service users, colleagues |
| Service Area | 4. Who are you collecting information from? |  | e.g. service users, relatives or representatives of service users |
| Service Area | 5. Will the project collect new personal data items which have not been collected before? |  |  |
| Service Area | 6. Will the project use existing information held by RDaSH in a different way? |  | RDaSH has a standard overarching privacy notice which explains how we use information. If this doesn’t cover new uses of information, we may need to give data subjects a new privacy notice. |
| Service Area | 7. Please tick the categories of personal information that will be held / used for this project | Name  Address  Postcode  Date of Birth  Emergency Contact/Carer’s details  NHS Number  Gender  GP / Consultant  Geographical Location/ IP Address  Occupation  Images | Personal data only includes information relating to natural persons who: can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.  Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.  Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but **it is still personal data**. |
| Service Area | 8. Will you collect any special categories of data? | Health information  Data relating to criminal convictions and offences  race  ethnic origin  politics;  religion  trade union membership  genetics  biometrics (where used for ID purposes)  sex life; or sexual orientation. | Special categories of data are defined in the General Data Protection Regulation (GDPR) and require a higher level of protection |
| Service Area | 9. If the project involves privacy invasive technologies such as biometrics or facial recognition please give some further details |  | e.g. Smart cards, radio frequency identification (RFID) tags, locator technologies (visual surveillance, profiling, data mining) |
| Service Area | 10. The data of approximately how many individuals will be affected by this project / change? |  | Give an approximate figure |
| Service Area | 11. Please specify the reason why you are processing personal data to meet one of the conditions for processing under GDPR |  | For processing of information to be lawful under the GDPR, you need to identify a lawful reason for processing personal data. For the public sector this is normally for a statutory function or legal duty. Further information |
| Service Area | 12. If you are not processing information for a statutory reason are you relying **only** on individuals providing consent as a reason to process information? |  |  |
| Service Area | 13. How will individuals be informed of how we process their information and who it will be disclosed to? |  | e.g. verbal privacy notice, website privacy notice, paper privacy notice or leaflet | |
| Service Area | 14. Have you checked that you are only collecting information that is relevant, necessary and adequate for the purpose you need this information for? |  |  | |
| Service Area | 15. What measures will be put in place to ensure that data is accurate and up to date? |  | e.g. audit checks, peer checking | |
| Service Area | 16. Who will access the information? Please detail services, roles and organisations |  |  | |
| Service Area | 17. Will information be shared with third parties? |  |  | |
| Service Area | 18. Is a data sharing agreement or contract in place? Please provide a copy.  If, Yes please ensure the due diligence questionnaire is completed and returned (***link?***). |  |  | |
| Service Area | 19. Where will the information be stored / accessed? |  | e.g. on paper, on a network folder / drive, on a website, on a dedicated system | |
| Service Area | 20. Will any information be sent off site (i.e. a building or network not under the direct control of RDaSH)  If so, how will it be transferred? |  | e.g. Standard email, secure email such as .net, website, courier, hand delivery, post, telephone | |
| Service Area | 21. Will any information be passed to contractors or sub contractors |  | If information is passed to contractors, we need to establish if they are a data controller or processor & put contractual measures in place (see Q1 guidance) | |
| Service Area | 22. How long will information be held?  Is there a retention schedule in place which covers this information? |  |  | |
| Service Area | 23. Does the information involve new matching or linking of personal data with data in other collections? |  |  | |
| Service Area | 24. Are you transferring any personal and / or personal sensitive information outside the European Union? |  |  | |
| Service Area | 25. In the event of a data loss or breach, what procedures would be followed? |  |  | |

**Section 3 – For new systems or changes to systems e.g. apps, software, databases etc.**

***For software installation, please ensure the software application form is complete (appendix 1)***

|  |  |  |  |
| --- | --- | --- | --- |
| Supplier and Service Area | 1. Is there an Access Control Policy in place? |  | An Access Control Policy outlines permissions to access information, usually based on an individual’s job role. Granular permissions are desirable. |
| Supplier and Service Area | 2. Is there a full audit trail in place for the information? |  | i.e. a complete log of transactions, including viewing, amending or deleting data. Are logs in a common syslog format that can be processed by a Security Incident and Event Management (SIEM) System? |
| Supplier and Service Area | 3. Will there be public access to any part of the system to allow people to review and/or update their own information? |  | For example, a library service where users can renew books online. |
| Supplier and Service Area | 4. Is personal or sensitive data encrypted in transit and at rest? |  | What encryption strength is used? Are files encrypted or is the entire disk encrypted? How many keys are used and who is given a key, what record is kept of that, how often are keys changed, is there a spare key and how is this securely stored, is there an admin override key, how is access to this controlled and is use audited? |
| Supplier and Service Area | 5. Are passwords salted and hashed? |  | How are passwords stored? If the system creates passwords, confirm that those passwords are not stored in plain text anywhere. If the passwords ae encrypted, please confirm the technical process for their protection. |
| Supplier and Service Area | 6. Can records be suspended from processing? |  | How does your system handle suspensions and confirm what data associated with that account is deleted? |
| Supplier and Service Area | 7. If the system is hosted does the supplier have a certified ISMS such as ISO27001:2013? |  | SOC2 or SOC3 reports would also be desirable. |
| Supplier and Service Area | 8. Can retention and disposal policies be applied to records? |  | How does the system manage this process? Does it have an automated process application of retention policy and disposal of records? |

**Section 4 – Information Governance – Record below how compliance with each requirement of the GDPR will be achieved**

|  |  |
| --- | --- |
| Principle 1 – Information shall be processed lawfully, fairly and in a transparent manner | **LAWFUL** processing of personal data: (Q 11) Art. 6, 1,  (a) **Consent of the Data Subject**  (b) necessary for a contract with Data Subject or with a view to entering a contact  (c) necessary for a legal obligation other than contract  (d) necessary Vital Interests of Data Subject (life and death) or other individual  (e**) necessary for public task or public function**  (f) necessary for the legitimate interest of Controller or Third Party to whom data are disclosed except where there is unwarranted prejudice to the legitimate interests of the Data Subject. **NEED TO DO A BALANCING OF INTERESTS**  **FAIR** processing of personal data (e.g. outcome of processing non-discriminatory in general)  **TRANSPARENT** processing of personal data (providing the data subject with information about the processing) (Q 12) (Q 16) |
| Principle 2 – Information shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes | Personal data collected for specified, explicit and legitimate purpose and not further processed in an incompatible manner. (Q 2) (Q11, 11a) |
| Principle 3 – Information shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed | Adequate, relevant and limited to what is *necessary* in relation to the purposes for which they are processed (‘data minimisation’); (Q 7) (Q 8) (Q 13)  Good Practice checks in relation to the processing purpose:  Does the purpose need personal data?  Every item of personal data justified in terms of the purpose at all times the personal data are processed  Relevance to purpose is time dependent (Q 2) (Q 11) (Q 20) |
| Principle 4 – Information shall be accurate and, where necessary, kept up to date | Accurate and, where *necessary*, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.  Personal data are inaccurate if they are incorrect or misleading as to any matter of fact.  No obligation to keep all personal data up to date (only when this is necessary – e.g. taking action against the data subject)  Obligation will be on the controller to demonstrate accuracy (Q 14) |
| Principle 5 – Information shall be kept no longer than necessary | Personal data kept in a form which permits identification of data subjects for no longer than is *necessary* for the purpose(s) of the processing  Retention criteria re the *purpose* takes account of:  Fulfilling any legal/statutory retention requirements  Identifying business need for retention from experience  Archiving requirements considered carefully  Delete personal data as *necessary* (securely) and putting “deleted” personal data “*beyond use*”  If processing legitimised by consent/explicit consent then “*necessary*” attaches itself to the consent ground of Article 6 and data minimisation Principle (Q 20) |
| Principle 6 – Information shall be processed in a manner that ensures appropriate security of the personal data | Processed in a manner that ensures appropriate security of the personal data, including protection against *unauthorised* or *unlawful* processing and against *accidental* loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).  unlawful processing  unauthorised processing (*mainstream* *security, technical measures, user authentication, role based access*)  accidental factors (*e.g.* *business* *continuity planning*)  organisational measures (e.g. *policies, management*)  technical measures (e.g. *encryption, access control)*  *(Section 3 New ICT Systems) (Q 15 – 19)* |
| Individuals Rights   1. The right to be informed 2. The right of access 3. The right to rectification 4. The right to erasure 5. The right to restrict processing 6. The right to data portability 7. The right to object 8. Rights in relation to automated decision making and profiling.   Detail how these will be met if applicable. | e.g. Individuals are informed about the rights in the privacy notice and provided with contact details for the Data Protection Officer. |

**Section 5 – Risk Assessment – To be completed by Information Governance**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Question No.** | **Risk identified** | **Risk Level** | **Proposed Solutions** | **Solutions completed** | **Risk Level after solutions applied** | **Evaluation – is the residual risk justified and proportionate to the aims of the project?** | **Evaluation – do we need to seek ICO approval? (residual risk high)** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Section 6 - Sign Off (Only sign off after identified risk solutions are completed)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role** | **Name** | **Signature** | **Date** |
| Project Manager / Service sign off (Name, signature & date) |  |  |  |
| Information Asset Owner (Head of Service) sign off (Name, signature & date) |  |  |  |
| Service Director sign off (Name, signature & date)  **Director Approval is required for systems or processes that incur a cost, require an approved budget or require approval for clinical use.** |  |  |  |
| Information Governance sign off (Name, signature & date) |  |  |  |
| IT Compliance & Security Advisor (Name, signature & date) |  |  |  |
| Data Protection Officer sign off (Name, signature & date) |  |  |  |

**In some circumstances the DPIA will need to approved by either the SIRO or Caldicott Guardian before processing commences**

|  |  |  |  |
| --- | --- | --- | --- |
| Date sent to SIRO | SIRO Advice | Approval | Completion Date |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Date sent to Caldicott Guardian | Caldicott Guardian Advice | Approval | Completion Date |
|  |  |  |  |

**If residual risk remains high after mitigating actions applied the DPIA will need to be sent to the Information Commissioner’s Office for approval before processing commences**

|  |  |  |  |
| --- | --- | --- | --- |
| Date sent to ICO | Advice from ICO | Approval | Completion Date |
|  |  |  |  |
| DPIA published | Sections to be published | Where Published (link) | Completion Date |
|  |  |  |  |

Appendix 1

**Software Installation - Screening questions**

**To be completed by the Service Area -** These questions will determine whether a DPIA is necessary. If the answer is ‘yes’ to any of the following questions you will need to complete a Data Protection Impact Assessment. Contact: [rdash.ig@nhs.net](mailto:rdash.ig@nhs.net) or Tel: 01302 796189

Completed Software Installation forms should be sent to [ITsupport.rdash@nhs.net](mailto:ITsupport.rdash@nhs.net)

|  |  |  |
| --- | --- | --- |
|  | Will the project involve the collection or use of personal information? |  |
|  | Will the project compel individuals to provide information about themselves? |  |
|  | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information (including RDaSH colleagues)? |  |
|  | Are you using information about individuals for a purpose it is not currently used for or in a way it is not currently used? |  |
|  | Does the project involve you using new technology which might be perceived as being particularly privacy intrusive? E.g. Use of biometrics or facial recognition? |  |
|  | Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? |  |
|  | Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? E.g. Health records, criminal records or other information that people would consider particularly private? |  |
|  | Will the project require you to contact individuals in ways which they may find particularly intrusive? |  |
|  | Does the project involve processing large volumes of personal data or data about a large number of individuals? |  |
|  | Does the system have a cost? |  |
|  | Does the system have an approved budget? |  |
|  | Is a contract required for the system?  If, Yes please ensure the due diligence questionnaire is completed and returned. |  |

**Section 1 - Project Details**

|  |  |  |
| --- | --- | --- |
| Project name/ title: |  | |
| Originator/Project Manager | Name |  |
| Title |  |
| Dept. & Team |  |
| Telephone |  |
| Information Asset Owner | Name |  |
| Title |  |
| Dept. & Team |  |
| Telephone |  |
| Director Approval  **Director Approval is required for systems or processes that incur a cost, require an approved budget or require approval for clinical use.** | Name |  |
| Title |  |
| Dept. & Team |  |
| Telephone |  |
| Describe the project or new system |  | |
| Why is this change required and what benefits will it bring? |  | |
| Please describe the flow of the information, a flow diagram may be of assistance |  | |

**NOTE: Completion and sign off of a DPIA or Systems Installation process by the Information Governance (IG) or Information Technology (IT) departments, does not indicate approval of software applications on behalf of the organisation that provide clinical information, nor confirm the accuracy of clinical information contained within them.**

|  |  |  |  |
| --- | --- | --- | --- |
| Name of product |  | | |
| Requestor (RDaSH, GP, DCCG) |  | Requestor Location |  |
| Requested installation date | Click here to enter a date. | No. of installations / devices |  |
| Installation site(s) |  | Type of product |  |
| Company & Contact details: | | Technical support contact, details and technical support hours: | |
|  | |  | |
| Description of product: [What does the product do, provide all relevant details including any documentation] | | | |
|  | | | |
| Hardware Requirements: [Server \ Cloud; Pc requirements, hard drive space, memory Windows version, browser, .net, additional software] | | | |
|  | | | |
| Firewall requirements: [ Details of any URL \ ports that are required ] | | | |
|  | | | |
| Software Licensing: [Details of software licensing requirements. Can the software be installed via our Software Deployment tool (SCCM), are there annual renewals to be managed? How are the licences managed?] | | | |
|  | | | |
| Software updates: [Details of how the software will be updated, are Admin rights required, can this be done via SCCM] | | | |
|  | | | |
| Remote support: [Is the software required to be remotely managed, what application is used to complete this?] | | | |
|  | | | |

**Internal use**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Track-It number |  | | | Date | Click here to enter a date. | |
| Organisation | RDaSH | | | DCCG | Doncaster GPs | |
| TAG Date | Click here to enter a date. | | | Priority | Choose an item. | |
| CAB Date | Click here to enter a date. | | | Project Management | Yes | No |
| Licence Manager | Yes | No |
| Approval | Approved | | | Not approved | Information required | |
| Comments: |  | | | | | |
| Passed to | Choose an item. | | | | | |
| Notify | Service Desk | | Communications | | DCCG | GP |
| Add to Change Calendar | Yes | No | E-mail to required staff | | Yes | No |