|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Protection Impact Assessment (DPIA)**  **Name of Project/Service** | | | | | | | | | | | | |
| This assessment should be completed as part of the business case for all new information systems and processes which involve the use of personal sensitive data or will significantly change the way in which personal data is handled. | | | | | | | | | | | | |
| The DPIA should be sent to Caldicott Guardian/*IG Lead/SIRO* for review and approval  DPO advice may be useful at any stage, including:   * how to complete a particular section of the form * whether a full DPIA is necessary (Screening section) * possible measures and safeguards to mitigate risks.   The DPO must review the completed form and advise on whether processing should go ahead. | | | | | | | | | | | | |
| **New /Change of System/Project General Details** | | | | | | | | | | | | |
| 1. | Person completing this assessment: | | | Name: Dr A Razvi  Job Title: GP Managing Partner  Email:  Phone: 01512967990 | | | | | | | | |
| 2. | Name of the new system/process/project work to be undertaken: | | | Ardens | | | | | | | | |
| 3. | Responsible Lead (name & email address): | | | Dr Razvi | | | | | | | | |
| 4. | Background:  (Why is the new system/change required - The purpose and aims of this work) | | | Data validation • The Summary Report offers an overview of the number of patients with coding errors and their value in terms of unclaimed QOF income. •Detailed Report contains EMIS ID, Usual GP, and the clinical code that needs adding/changing for each individual patient. It includes instructions explaining how to easily replace the incorrect clinical code with the correct one. Ardens Starter, Plus and Pro • Ardens Starter Plus and Pro offer clear, concise, and intuitive templates that automatically adapt for individual patients based on the data within their clinical record. It includes templates for long-term conditions, QOF, enhanced services, frailty, and many other clinical areas. The templates are customi | | | | | | | | |
| 5. | List the main activities of the project: | | | As above | | | | | | | | |
| 6. | What are the intended benefits: | | | As above | | | | | | | | |
| 7. | Date new system, process or work to start: | | |  | | | | | | | | |
| 8. | Information Asset Owners  (All system/assets must have Information Asset Owners (IAO). IAO’s will be the Practice Manager or Partner GP  *This is the person who takes overall responsibility for this asset, and may do so for several other assets. The IAO is responsible for reporting any breaches that happen with their assets to the SIRO, as well as identifying and mitigating any risks to the asset, and deciding which users have access to it.* | | | Name: | | | | Dr A Razvi | | | | |
| Title: | | | | GP Managing Partner | | | | |
| Department: | | | |  | | | | |
| Telephone: | | | |  | | | | |
| Email: | | | |  | | | | |
| 9. | Who is the Information Asset Administrator  *The IAA is an operational staff member who has day to day responsibility for ensuring that the asset is secure and that those who should be able to access it are able to do so*. | | | Name: | | | | Ann Fraser | | | | |
| Email: | | | | Ann.Fraser@livgp.nhs.uk | | | | |
| 10. | Date DPIA was completed: | | |  | | | | | | | | |
| **DPIA Screening** | | | | | | | | | | | | |
| Screening Questions | | | | | | Yes/No | | | | Comments | | |
| 11. | Will the project involve the collection of new information about individuals? | | | | | **no** | | | |  | | |
| 12. | Will the project compel individuals to provide information about themselves? | | | | | **no** | | | | Access to personal confidential data is restricted by RBAC codes | | |
| 13. | Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? | | | | | **no** | | | |  | | |
| 14. | Do you propose using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? | | | | | **no** | | | |  | | |
| 15. | Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition | | | | | **no** | | | |  | | |
| 16. | Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? | | | | | **no** | | | | The provision of health and social care | | |
| 17. | Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? E.g. health records, criminal records or other information that people would consider to be particularly private? | | | | | **no** | | | | Personal confidential data is not used | | |
| 18. | Will the project require you to contact individuals in ways which they may find intrusive? | | | | | **no** | | | |  | | |
| 19. | Will the project store information using cloud technology? | | | | | **no** | | | |  | | |
| 20. | Will the project transfer information outside the European Economic Area (EEA)? | | | | | **no** | | | |  | | |
| * If you answered **no** to all the questions, you **DO NOT** need to proceed to a full Data Protection Impact Assessment. Save this document to evidence your assessment * If you answered **yes** to any of these questions, you **DO** need to proceed to a full Data Protection Impact assessment. Complete the following sections and save to evidence your assessment | | | | | | | | | | | | |
| **Full Data Protection Impact Assessment** | | | | | | | | | | | | |
| 21. | Who are the Data Subjects? (e.g. the people whose data will be held/processed in this new system – this may be patients and/or staff) | | |  | | | | | | | | |
| 22. | What Data Classes will be held on this system (i.e. the actual data fields) split by Personal and Special Category | | | Personal Data: | | | | | | | | |
| Special Category Data: | | | | | | | | |
| 23. | Children (those under 13 years of age)  Does the project involve internet services of any kind, with regards to children? | | |  | | | | | | | | |
| 24. | If yes, are you planning to gain and record consent? How will you achieve this? | | |  | | | | | | | | |
| 25. | If the child is under 13 years of age, will you gain and record the parents’ consent? If Yes how will you achieve this? | | |  | | | | | | | | |
| 26. | Will this system/process include data which was not previously collected? | | |  | | | | | | | | |
| 27. | Have you assessed the likelihood of data causing any unwarranted distress or damage to individuals concerned? | | |  | | | | | | | | |
| 28. | Is there a legal basis for holding and processing this data? | | | Article 6(1) Lawfulness of processing: | | | | | | | | |
| Article 9(2) Processing of special categories of personal data: | | | | | | | | |
| 29. | Does the system/process include new or amended identity authentication requirements that may be intrusive? | | |  | | | | | | | | |
| 30. | What checks have been made regarding the adequacy, relevance and necessity of data used? | | |  | | | | | | | | |
| 31. | Can the system/process use pseudonyms or work on anonymous data? | | |  | | | | | | | | |
| 32. | Can the data subjects opt-out of their data being added to the system/used by the process, and if so is this publicised? | | |  | | | | | | | | |
| 33. | Does the Fair Processing Notice (or Privacy Notice on the practice’s public website cover your planned activity | | |  | | | | | | | | |
| 34. | Who are the partners for the data sharing? | | |  | | | | | | | | |
| **Data Security** | | | | | | | | | | | | |
| 35. | Will the system require the use of the practice computer equipment? If so has the Informatics Merseyside (IM) IT Security Team been informed and assessed the system? | | |  | | | | | | | | |
| 36. | Who will use the system/process and have access to the data? | | |  | | | | | | | | |
| 37. | Have or will areas involved completed the Data Security Awareness module | | |  | | | | | | | | |
| 38. | Will the data be shared with any other organisations?  (check privacy policy of provider/Sharing Agreements for details) | | |  | | | | | | | | |
| 39. | Where will data be held? | | |  | | | | | | | | |
| 40. | What format will data be stored in? | | |  | | | | | | | | |
| 41. | Does the system / process change the way data is stored? | | |  | | | | | | | | |
| 42. | How will staff access and amend data? | | |  | | | | | | | | |
| 43. | How will data be shared?  e.g. email, NHS mail, internal/external post, phone, website transfer, mesh, sms | | |  | | | | | | | | |
| 44. | Are you transferring any personal and / or sensitive data to a country outside the European Economic Area (EEA)? | | | Yes  No  *If yes, please outline the data types, flow (sending/receiving), country, transfer methods and any measures in place to ensure adequate levels of security when transferred (in transit)to this country.* | | | | | | | | |
| 45. | Description of information flows (either words or diagram) | | |  | | | | | | | | |
| 46. | What security measures have been taken to protect the data? (request 3rd party security whitepapers or documentation for system)  Please include access control, data security in transit and encryption in the answer | | |  | | | | | | | | |
| 47. | Is there a useable audit trail in place for the asset? *For example, to identify who has accessed a record* | | |  | | | | | | | | |
| 48. | How often will the system/process be audited? | | |  | | | | | | | | |
| 49. | Who supplies the system/process? | | |  | | | | | | | | |
| 50. | Is the supplier of the system/recipient of the data registered with the ICO? (please give registration number) | | |  | | | | | | | | |
| 51. | If third party supplier are they based within the EEA | | |  | | | | | | | | |
| 52. | Where will the 3rd party store the data? (full addresses) | | |  | | | | | | | | |
| 53. | Has the organisation completed the Data Security and Protection (DSP)Toolkit to a satisfactory level? | | |  | | | | | | | | |
| 54. | Does the contract include necessary IG clauses? | | |  | | | | | | | | |
| 55. | What business continuity plans are in place in the case of data loss / damage as a result of human error / computer virus / network failure / theft / fire / flood / other disaster?  (for the practice) | | |  | | | | | | | | |
| **Data Quality** | | | | | | | | | | | | |
| 56. | Who provides the information for the asset? | | |  | | | | | | | | |
| 57. | Who inputs the data into the system? | | |  | | | | | | | | |
| 58. | How will the information be kept up to date and checked for accuracy and completeness? | | |  | | | | | | | | |
| 59. | Can an individual (or a court) request amendments or deletion of data from the system? | | |  | | | | | | | | |
| **On-Going Use of Data** | | | | | | | | | | | | |
| 60. | Will the data be used to send direct marketing messages? | | |  | | | | | | | | |
| 61. | If yes, are consent and opt-in procedures in place? | | |  | | | | | | | | |
| 62. | Does the system/process change the medium for disclosure of publicly available information? | | |  | | | | | | | | |
| 63. | Will the system/process make data more readily accessible than before? | | |  | | | | | | | | |
| 64. | What is the data retention period for this data? *(please refer to* [*Records Management for Health & 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) ) | | |  | | | | | | | | |
| 65. | How will the data be destroyed when it is no longer required? | | |  | | | | | | | | |
| 66. | Does your disaster recovery solution use 3rd party supplier? | | |  | | | | | | | | |
| 67. | Please provide details of all accreditations the supplier holds  e.g. ISO27001 | | |  | | | | | | | | |
| 68. | Has your Disaster Recovery Plan been tested and was all data retained and secure? | | |  | | | | | | | | |
| **Identify and Assess Risks** | | | | | | | | | | | | |
| Information security risks should be highlighted to the IM IT Security Team to complete any necessary risk assessments on new systems or changes to existing systems.  Any issues that may arise could adversely impact other organisations and services hosted by Informatics Merseyside, because of this the IM IT Security Team need to complete their assessment before the system can be commissioned for use. | | | | | | | | | | | | |
| **Risk Description (**source of risk and nature of potential impact **to individuals, the Practice, CCG or to wider compliance)** | | | | **Likelihood of harm**  (Remote, possible or probable) | | | **Severity of harm**  (minimal, significant or severe) | | | | **Overall risk**  (low, medium or high) | |
|  | | | |  | | |  | | | |  | |
|  | | | |  | | |  | | | |  | |
|  | | | |  | | |  | | | |  | |
|  | | | |  | | |  | | | |  | |
|  | | | |  | | |  | | | |  | |
| **Identify Measure to Reduce Risk** | | | | | | | | | | | | |
| **Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in the table above** | | | | | | | | | | | | |
| **Risk** | | **Proposed Risk Solution** (reduce or eliminate risk) | | | **Effect on risk**  (Is the risk reduced, transferred, accepted) | | | | **Remaining risk**  (Low, medium or high) | | | **Measure approved**  (Yes/No) |
|  | |  | | |  | | | |  | | |  |
|  | |  | | |  | | | |  | | |  |
|  | |  | | |  | | | |  | | |  |
|  | |  | | |  | | | |  | | |  |
| **DPIA Sign Off** | | | | | | | | | | | | |
| Item | | | Name/Date – June 2021 | | | | | | Notes | | | |
| SIRO approved: | | | Name:Dr Razvi | | | | | | *Integrated actions back into project plan, with date and responsibility for completion* | | | |
| Date: | | | | | |
| Caldicott Guardian approved: | | | Name: Dr Razvu | | | | | | *If accepting any residual high risk, consult the ICO before going ahead* | | | |
| Date: | | | | | |
| DPO advice provided | | | Name:Dr Razvi | | | | | | *DPO should advise on compliance, Identify measure to reduce risk section and whether processing can proceed* | | | |
| Date: | | | | | |
| Summary of DPO advice: | | | | | | | | | | | | |
| DPO advice accepted or overruled by:  (SIRO/Caldicott Guardian) | | | Name: | | | | | | *If overruled, you must explain your reasons* | | | |
| Date: | | | | | |
| Comments: | | | | | | | | | | | | |
| Consultation responses reviewed by: | | | Name: | | | | | | *If your decision departs from individuals’ views, you must explain your reasons* | | | |
| Date: | | | | | |
| Comments: | | | | | | | | | | | | |
| This DPIA will be kept under review by: | | | Name: | | | | | | *The DPO should also review ongoing compliance with DPIA* | | | |
| Date: | | | | | |