|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Protection Impact Assessment (DPIA)**  **MediData Exchange Limited eMR** | | | | | | | | | | | | |
| 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. | | | | | | | | | | | | |
| \*\*Practice can amend this paragraph to reflect their process (created as part of the DSP Toolkit 18/19)  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 | | | | | | | | | | | | |
| **Overview** | | | | | | | | | | | | |
| **1.** | | **Name of the new system or process:** | | | Medi2Data eMR  MediData Exchange Limited | | | | | | | |
| **2.** | | **Responsible Lead (name & email address):** | | | Dr A Razvi. GP Managing Partner. | | | | | | | |
| **3.** | | **What are the main aims?** | | | Complete Subject Access Requests (SARs) using Medi2Data eMR redaction software | | | | | | | |
| **4.** | | **List the main activities of the project:** | | | eMR – to ensure all Subject access requests are dealt with in a timely manner. | | | | | | | |
| **5.** | | **What are the intended outcomes?** | | | To ensure all SARs are redacted to the appropriate degree and dealt with in a timely manner | | | | | | | |
| **Information Asset Register** | | | | | | | | | | | | |
| **6.** | | **Who is the Information Asset Owner – IAO (Name & email address) -** | | | *Dr A Razvi* | | | | | | | |
| **7.** | | **Who is the Information Asset Administrator - IAA (name & email address)** | | | *Sophie Whittaker* | | | | | | | |
| **Data** | | | | | | | | | | | | |
| **8.** | | **Who are the Data Subjects? (e.g. the people whose data will be held in this new system – this may be patients and/or staff)** | | | Patients registered at the GP Practice | | | | | | | |
| **9.** | | **What Data Classes will be held on this system (i.e. the actual data fields)?** | | | All data classes will be held as the nature of a Subject Access Request (SARs) this will be both personal and special category data | | | | | | | |
| **10.** | | **Will this system/process include data which was not previously collected?** | | | No | | | | | | | |
| **11.** | | **Have you assessed the likelihood of data causing any unwarranted distress or damage to individuals concerned?** | | | *yes* | | | | | | | |
| **12.** | | **Is there a legal basis for holding and processing this data?** | | | *For the use of Medi2Data eMR to produce Subject Access Requests the legal basis relied upon will be consent;*  ***Article 6***  **Lawfulness of processing**  (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;  ***Article 9***  **Processing of special categories of personal data**  (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; | | | | | | | |
| **13.** | | **Does the system/process include new or amended identity authentication requirements that may be intrusive?** | | | No | | | | | | | |
| **14.** | | **What checks have been made regarding the adequacy, relevance and necessity of data used?** | | | *All checks performed by DPO confirm relevance and adequacy of the data that is redacted and sent securely to Insurance companies/ solicitors.* | | | | | | | |
| **15.** | | **Can the system/process use pseudonyms or work on anonymous data?** | | | No, the nature of a SAR’s is that the information is identifiable about an individual, 3rd party data should be redacted | | | | | | | |
| **16.** | | **Can the data subjects opt-out of their data being added to the system/used by the process, and if so is this publicised?** | | | *Yes* | | | | | | | |
| **17.** | | **Who are the partners for the data sharing?** | | | Yew Tree Medical Centre  MediData Exchange Limited  Patient | | | | | | | |
| **Data Security** | | | | | | | | | | | | |
| **18.** | **Who will use the system/process and have access to the data?** | | | | Administrative Staff  MediData staff have no access to medical data, they use the latest encryption methods as per industry standards. Storage of the customer’s encrypted data is in a UK, tier 4 data centre with the strictest security processes and policies. The site has 24x7 security and multiple entry checkpoints to prevent unauthorised access. | | | | | | | |
| **19.** | **Have or will areas involved completed Data Security Awareness module** | | | | All Staff Complete Mandatory Data Security Awareness Level 1Training on an annual basis  MediData staff complete Data Security Awareness training annually | | | | | | | |
| **20.** | **Will the data be shared with any other organisations?** | | | | No | | | | | | | |
| **21.** | **Where will data be held?** | | | | Metadata and limited information is stored in MediData Exchange Limited application database, Some information, including redacted files may be stored in PDF/Document format within their infrastructure, all which uses industry standard encryption.  All infrastructure is Privately Hosted, single tenancy. The Data Centres (DC) are operated by a large uk-based plc. The DC infrastructure is currently based in Maidenhead, Berks, but have locations across the country and the plan will be to have multi-site operations.  Data at rest:  Data is stored on hardware which is dedicated to MediData. Encryption is used across the infrastructure on data storage volumes.  **Data Flow** The core principal relating to the data flow is that data is only stored where it is authorised to be; within the GP Operating System (EMIS), within MediData’s application or with MediData’s client’s systems. It is never downloaded to a GP surgery or MediData staff device, e-mailed or produced in hard copy during the process of completing a request.  The data flow, through using the application, is as follows:   1. **MediData Client raises a request** MediData’s client raises a request for a medical report, through MediData’s application(portal), MDx. This information will include personal information about the patient. This data is stored within MediData’s application. 2. **Request is raised with the patient’s GP** MediData’s application will raise a request which will be sent through to the patient’s GP. The GP will be notified with limited information and will be required to login to the MediData application to retrieve the request in full 3. **Request is completed** The patient’s GP will then process the request within MediData’s application drawing information in from the GP Operating System (EMIS) in redacted form. The GP will then manually review the form amending / adding anything relevant to the request before signing off the report within MediData’s application 4. **Complete report is returned to the client** Notification of a completed report is sent to MediData’s client. The client would then login to MediData’s application and review / download the completed report. As the medical report moves from “finalising to completed stage”, a secure web link is sent to the email address of the patient - entered by the surgery.   Dual factor authentication is used, by which, upon receipt of that email a button has to be clicked to activate the text code – this is sent only to the contact number that the surgery has entered. | | | | | | | |
| **22.** | **What format will data be stored in?** | | | | MediData Uses the latest encryption methods as per industry standards. Storage of the customer’s encrypted data is in a UK, Tier 4 data centre. | | | | | | | |
| **23.** | **Does the system / process change the way data is stored?** | | | | Yes­ | | | | | | | |
| **24.** | **How will staff access and amend data?** | | | | *Via the eMR software/ website* | | | | | | | |
| **25.** | **How will data be shared?** | | | | Practice data is only ever shared with permission and MediData cannot allow this without express permission from you.  Data Transit:  All data transit occurs via HTTPS connections with 3rd party certificate authentication. | | | | | | | |
| **26.** | **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, country, transfer methods and any measures in place to ensure adequate levels of security when transferred to this country.* | | | | | | | |
| **27.** | **What security measures have been taken to protect the data?** | | | | eMR is an application when interfaced with EMIS web within the HSCN / NHS secure environment allows through the API calls specific data to be pulled from the EMIS system into an eMR generated subject access request or insurance report .  This interface can only happen following a GP surgery setting up eMR through the EMAS (administration) access of the EMIS clinical system of which we are an accredited 3rd party.  No extraction of data takes place outside this secure infrastructure (HSCN)  Infrastructure utilises industry standard techniques in terms of network server security.  All data stored within the infrastructure is stored in encrypted forms.  All infrastructure is Privately Hosted, single tenancy. The Tier 4 DCs are operated by a large UK-based plc. The DC the infrastructure is currently based in is in Maidenhead, Berks, but they have locations across the country and the plan will be to have multi-site operations.  **Accreditations** Across Medidata’s infrastructure, business and partners the following accreditations apply.   1. **BS 25999-2**– Business Continuity Management 2. **Cyber Essentials** – Cyber Security self-assessment 3. **HSCN Compliance**– Health & Social Care Network Compliance 4. **ISO 9001** – Quality Management System 5. **ISO 14001**– Environmental Management System 6. **ISO 20000** – IT Service Management 7. **ISO 22301** – Societal Security / Business Continuity System 8. **ISO 27001**– Information Security Management System 9. **OHAS 18001**– Health & Safety Management System 10. **PCI DSS Compliance** – Payment Card Industry Data Security Standard | | | | | | | |
| **28.** | **Is there a useable audit trail in place for the asset?** *For example, to identify who has accessed a record* | | | | Yes , Medi2Data eMR tracks all changes in the system and any medical reports created are stored with a unique reference number | | | | | | | |
| **29.** | **How often will the system/process be audited?** | | | | *yearly*  MediData has 3rd party suppliers who regularly audit and review our security measures, to ensure they are consistently remaining rigorous, and keeping up with industry standards. | | | | | | | |
| **30.** | **Who supplies the system/process?** | | | | MediData Exchange Limited | | | | | | | |
| **31.** | **Is the supplier of the system/recipient of the data registered with the ICO? (please give registration number** | | | | MediData Exchange Limited -  ICO registration Number: ZA353121  *Yew Tree Medical Centre - Z4781122* | | | | | | | |
| **32.** | **Has the organisation completed the NHS Digital DSP Toolkit to a satisfactory level?** | | | | MediData completed accreditation for IG Toolkit 2017and 2018,  Data Security and Protection Toolkit 2019 - Last published 01/04/2019  NHS Digital ODS Code is 8JQ49  Yes – YewTree Medical Centre completes this annually | | | | | | | |
| **33.** | **Does the contract include necessary IG clauses?** | | | | Yes | | | | | | | |
| **34.** | **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?** | | | | As per the Business continuity policy  MediData have strict policies and procedures in place –   * Risk Register * Information Security Governance Policy * MediData eMR Data Security System Counter measures   All these policies are constantly reviewed and updated.  They are however strictly confidential to the Organisation and cannot be shared externally. | | | | | | | |
| **Data Quality** | | | | | | | | | | | | |
| **35.** | | **Who provides the information for the asset?** | | | In the context of using eMR for a SAR the Data is controlled an managed by Primary Care GP Practice | | | | | | | |
| **36.** | | **Who inputs the data into the system?** | | | Sophie Whittaker & Khadijah Abidi | | | | | | | |
| **37.** | | **How will the information be kept up to date and checked for accuracy and completeness?** | | | *Regular audits* | | | | | | | |
| **38.** | | **Can an individual (or a court) request amendments or deletion of data from the system?** | | | Requests can be made, these will be reviewed on individual basis and if found to be appropriate for amendment/deletion | | | | | | | |
| **On-Going Use of Data** | | | | | | | | | | | | |
| **39.** | | **Will the data be used to send direct marketing messages?** | | | No | | | | | | | |
| **40.** | | **If yes, are consent and opt-in procedures in place?** | | | N/A | | | | | | | |
| **41.** | | **Does the system/process change the medium for disclosure of publicly available information?** | | | No | | | | | | | |
| **42.** | | **Will the system/process make data more readily accessible than before?** | | | Yes | | | | | | | |
| **43.** | | **What is the data retention period for this data?** *(please refer to the Records Management for Health & Social Care 2016)* | | | Deleted automatically after the expiry of the 6 months access period ends | | | | | | | |
| **44.** | | **How will the data be destroyed when it is no longer required?** | | | *Emails are deleted on a regular basis*  MediData - The data is automatically wiped from the system and is never retrievable. As it is not physical data all we need to do is simply remove it from our records | | | | | | | |
| **45.** | | **Does your disaster recovery solution use a 3rd party supplier?** | | | MediData Business Continuity / DR  All servers running MediData’s applications are regularly and automatically backed up. The physical infrastructure running the application environment will have additional hosts added during production rollout to provide high availability in the event of hardware failure | | | | | | | |
| **46.** | | **Does your Disaster Recovery provider have any accreditations e.g. ISO27001** | | | Yes please see - <https://www.iomart.com/about-iomart/accreditations/> | | | | | | | |
| **47.** | | **Has your Disaster Recovery Plan been tested and was all data retained and secure?** | | | Yes scheduled imaging processes automatically back up all data. | | | | | | | |
| **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) | |
| There is the potential for a data breach to occur if the eMR portal is accessed by Practice staff on non IM provisioned equipment. IM cannot guarantee the security on staff personal devices. | | | | | | Possible | | | Significant | | Medium | |
|  | | | | | |  | | |  | |  | |
|  | | | | | |  | | |  | |  | |
| **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) |
| There is the potential for a data breach to occur if the eMR portal is accessed by Practice staff on non IM provisioned equipment. IM cannot guarantee the security on staff personal devices. | | | Multi factor authentication (SMS or email one time password) is needed when accessing the portal from a non-NHS site. eMR can remove the practice phone number and email from their registration, which would prevent them from logging into the portal when not on site. | | | | Reduced | | | Low | |  |
| There is the potential for a data breach to occur if the eMR portal is accessed by Practice staff on non IM provisioned equipment. IM cannot guarantee the security on staff personal devices. | | | Policy to state that only Trust issued equipment is to be used to access systems that hold practice data. | | | | Reduced | | | Medium | |  |
|  | | |  | | | |  | | |  | |  |
|  | | |  | | | |  | | |  | |  |
| **DPIA Sign Off** | | | | | | | | | | | | |
| Item | | | | Name/Date | | | | Notes | | | | |
| SIRO approved: | | | | Name: Dr A Razvi | | | | *Integrated actions back into project plan, with date and responsibility for completion* | | | | |
| Date: September 2019 | | | |
| Caldicott Guardian approved: | | | | Name: Dr A Razvi | | | | *If accepting any residual high risk, consult the ICO before going ahead* | | | | |
| Date: September 2019 | | | |
| DPO advice provided | | | | Name: Dr A Razvi | | | | *DPO should advise on compliance, Identify measure to reduce risk section and whether processing can proceed* | | | | |
| Date: September 2019 | | | |
| 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* | | | | |