**dATA Protection Impact Assessment**

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

*This DPIA template must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled or processed.*

|  |  |  |
| --- | --- | --- |
| **Project / Work Stream Name** | Folkestone, Hythe and Rural Primary Care Network  PCN Hub Operating Model (“the pilot”) | |
| **Project / Work Stream Leads and Consultants** | Name(s) | 1. Andy Gove 2. Dr Aravinth Balachandran |
| Designation | 1. Digital Transformation Manager 2. Clinical Director   Folkestone, Hythe and Rural PCN |
| Telephone | 01303 235 314 |
| Email | 1. [andrew.gove@nhs.net](mailto:andrew.gove@nhs.net) 2. [abalachandran@nhs.net](mailto:abalachandran@nhs.net) |
|  | Information Asset Owner | Folkestone, Hythe and Rural Primary Care Network  Lead Practice: G82016 Oaklands Health Centre |
| **Version Control:** | |  |  |  | | --- | --- | --- | | Date | Name | Designation | | 13/07/2023 | Latifa Aina | (External) DPO | |  |  |  | |  |  |  | | |
| **Timeframe of the project (if known):** | A full deployment of this pilot is launched in completed Q1 2023.  Should this pilot project prove to be a success, it is intended that this approach will provide a framework operating model that can be applied to other Primary Care Networks across the country that want to work this way. | |
| **Overview:**  **Description of the purpose of the project/work stream and how is the processing of information necessary to that work?** | The purpose of this project is to stand up a PCN Hub operating model to deal with Primary Care demand across the seven practices within Folkestone, Hythe and Rural PCN (FHR PCN) efficiently, safely and effectively at a PCN centralised hub level. The main objectives of the project are to:   1. Federate online consultation triage by using the e-consult portal – allowing all online consultations from the x7 constituent practices to be delivered into a hub specific clinical system where they will be triaged and passed to the relevant team for action. This is the ‘Hub element of the PCN Hub.’ 2. Host staff that need to consult with patients from across the footprint of the PCN within a hub clinical system, which can be accessed via single sign-on with access to the patient’s registered GP record maintained by any of the 7 member practices of the PCN. 3. Hold a central appointment book within a hub clinical system that is accessible by all constituent practices in order to provide seamless access to PCN level services. 4. Provide a single point of access to proactively manage PCN level service delivery.   At the centre of the PCN hub operating model will be the PCN specific EMIS Clinical Service, which will be configured to have a series of bi-directional one to one EMIS to EMIS technical sharing agreements with the EMIS Web system, which is utilised by each PCN practice, rather than a many to many technical sharing agreements. A dedicated administrative and clinical team will support the planned PCN Hub operating model.  In addition to the practice-to-practice technical data sharing agreement outlined above, the PCN EMIS Clinical system will utilise ‘Consultation Write Back’ functionality to update a patient’s GP record with any record entries completed by PCN level healthcare services. This functionality uses a technical data sharing agreement to ‘copy’ a consultation completed within the PCN EMIS Clinical Service back to the patient’s EMIS Web hosted GP record at a constituent GP practice. The information that is written back to patient’s GP record is clinically coded.  The implementation of the PCN Hub Operating model outlined above requires the registration of a patient within the PCN EMIS Clinical Service. This will create a PCN level record for the patient that will then be used to record consultations conducted by PCN level services. Technical capabilities within the EMIS Clinical Service are used to register, or ‘trace’ the patient into the system and create a new registration under a ‘Community’ registration type. At go-live a ‘Patient Trace’ technical capability was initially used to create a new PCN level patient record. Due to the steady increase in the number of patients now being consulted with at PCN level manual registrations are no longer viable and there is now a requirement to utilise an EMIS managed service to complete a bulk demographic registration of all fully registered GP practice patients from all Folkestone, Hythe & Rural PCN within the EMIS Clinical Service. This will improve the efficiency of PCN healthcare service delivery and reduce the risk of human error when patients are registered via the ‘Patient Trace’ route.  **Process – PCN level healthcare service:**   1. In a typical patient journey, the patient’s registered GP practice upon triage may deem a patient suitable for referral into one of the PCN healthcare services. 2. The patient will be referred into the PCN healthcare service via one of two means:    1. Using the practice EMIS web to make a cross organisational appointment booking into the PCN Hub clinical system appointment book.    2. Using the practice clinical system (EMIS web) to make a direct referral into the PCN Hub clinical system, which is received in the ‘Workflow’ module. 3. The patient’s registered GP communicates details of the referral, and any associated appointment, to the patient via SMS or telephone call. 4. The PCN healthcare service will register the patient within the PCN hub clinical system and consult against the record as required. 5. Any consultation entered into the patient’s PCN hub clinical system record will be sent back to the patient’s registered GP record in coded form.   **Process – PCN federated online consultation triage:**   1. Patients complete an online consultation via the website of their registered GP practice or using the NHS App. 2. Upon completing the online consultation is sent securely onto the following clinical systems:    1. The PCN Hub clinical system    2. The eConsult Smart Inbox triage tool (completed DPIA for this is available here 3. A clinical triage of the online consultation will be completed by a dedicated PCN team. 4. If appropriate, the patient will be offered an appointment with a PCN healthcare service. 5. If the patient’s presenting condition is not suitable to be managed by a PCN Hub healthcare service, or the patient refuses an appointment with a PCN Hub healthcare service, the patient will be passed back to the practice to manage. 6. An administrative team will register the patient within the PCN Hub clinical system and attach the online consultations to the patient’s record. This will be automatically added to the patient’s GP record. 7. Any consultation entered into the patient’s PCN hub clinical system record will be sent back to the patient’s registered GP record in coded form.   The PCN hub clinical system will be:   * SPINE enabled. * Has its own PCN Registration Authority (smart card) services. * Has EPS enabled an associated PCN level prescribing cost centre. * PDS enabled. * Summary care record enabled. * MESH enabled. * GP Connect enabled. * Has full suite of Ardens templates and searches. * Has integrated CPCS module – PCN configured. * Integrated eConsult Toolbar and eConsult Smart Inbox – PCN configured. * Integrated accuRx – PCN configured. * Integrated Docman Share app (Docman Share Viewer) – PCN configured. * Integrated iPlato messaging system – PCN configured for patient appointment management (reminders & cancellations)   All the above will ensure at a PCN level, all available patient’s information is viewable (read only) to have a full medical history at any time. This has in scope the full coded record, associated free text entries, medications etc as well as attachments to the patient’s record.   1. Consultation notes recorded when patients are consulted with within the PCN Hub clinical system are automatically fed back to their clinical record at their registered GP practice and forms part of their consultation notes.    Summary of the list of services that the PCN hub will host:   1. PCN Minor Illness Service (staff employed directly by PCN practices) 2. PCN Central Online Consultation Processing (staff employed directly by PCN practices) 3. PCN Dietician (Contracted to Xcel Health) 4. PCN Hosted ARRS services, including:  * Social Prescribing Link Workers (employed directly by a PCN practice) * Cancer Care Coordinators (employed directly by a PCN practice) * MDT Coordinators (employed directly by a PCN practice) * Clinical Pharmacists (employed directly by a PCN practice) * First Contact Physiotherapy (Contracted to Ashford Therapy & Rehabilitation Alliance Ltd by PCN practice) * Mental Health Practitioner (Contracted to KMPT by PCN practice) * Occupational Therapist (Contracted to KCC by PCN practice) * PCN Care Home Team (team comprises of staff employed by a PCN practice either under the ARRS scheme or via direct contract of employment with a PCN practice)   PCN level configured Edenbridge Apex, Ardens Manager and associated searches, and EMIS Enterprise Searches & Reports will provide patient identifiable and/or non-identifiable data for the following:   * Population Health Management (PHM) as legally permitted and defined by NHS England * Activity (inc. hosted ARRS Services) * Medicines Management (inc. MHRA alerts) * QOF & IIF - running searches against an entire patient list to identify those affected by MHRA alerts for example, or to find a particular cohort of patients that require attention (may not have received a Flu jab for example).   Folkestone, Hythe & Rural PCN is signed up to [the data provision notice](https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/data-provision-notices-dpns/gp-appointments-data-collection-version-2.0) in order for NHS England to be able to receive an extract of the primary care appointment activity from the PCN Hub model. | |
| **Outcomes:**  **What will be the benefits or effects of the processing** *i.e., what actions/decisions will result from the processing?* | It is anticipated that patients will benefit from this operating model in the following ways:   * Improved access to Primary Care services (both via the online consultation route, and more traditional routes such as telephone and in-person presentation at practice) * Improved online consultation response time * More efficient online consultation processing * Better management of patients registered at PCN practices through the use of population health management tools | |
| **Information Asset** | Subject to the purpose and approach being agreed as necessary and proportionate, and data security and protection controls being appropriate and sufficient, it is proposed to use data held in the following Information Assets.   * Patients’ data as stored on each of the 7 GP Practices making the PCN’s clinical systems. * Data (consultation notes) taken at the PCN hub level into their EMIS will be flowed back into each Practice’s EMIS to form part of the patients’ medical records. Patients’ data (consultation notes) as entered into at PCN level will be maintained in the PCN EMIS clinical system for continuity and consistency of providing direct care to patients and propensity with the PCN becoming a data controller for that data (and all accompanying responsibilities that comes with that). This makes a compelling case for PCN to be statutorily recognised as legal entities under the lead practice model, this increases the risks /burden on the lead practice. | |
| **Environmental Scan**  **Describe the consultation/checks that have been carried out regarding this initiative or, project of similar nature, whether conducted within your organisation or by other organisations.**  *Please provide any supporting documents such as benefit study, fact sheets, white papers, reports or referenced articles published by industry associations, technology providers, and research centres*. | This is a pilot.  However, it is worth noting that FHR PCN hub will be the first of its type for the way in which the care record management will work –as the first PCN nationally to have the functionality in this way with NHS E Southeast Region Primary Care Transformation Programme intending to blueprint this. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Step 1: Complete the Screening Questions** | | | |
| **Q 1** | **Category** | **Screening question** | **Yes/No** |
| 1.1 | Technology | Does the project introduce new or additional information technologies that can substantially reveal an individual’s identity and has the potential to affect that person’s privacy? | Yes |
| 1.2 | Technology | Does the project introduce new or additional information technologies that can substantially reveal business sensitive information, specifically: have a high impact on the business, whether within a single function or across the whole business? | No |
| 1.3 | Identity | Does the project involve new identifiers, re-use or existing identifiers e.g., NHS or NI number, Local Gov. Identifier, Hospital ID no. or, will use intrusive identification or identity management processes or, electronic linkage of personal data? | Yes, the purpose remains the same, but the information will be processed in a new way – centrally rather than at each PCN practice |
| 1.4 | Identity | Might the project have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions? | No |
| 1.5 | Multiple organisations | Does the project involve multiple organisations, whether they are public sector agencies i.e., joined up government initiatives or private sector organisations e.g., outsourced service providers or business partners? | Yes, 7 data controllers and a number of digital system providers (all of which are already in use). |
| **Q** | **Category** | **Screening question** |  |
| 1.6 | Data | Does the project involve new process or significantly change the way in which personal data/special categories of personal data and/or business sensitive data is handled? | Yes |
| 1.7 | Data | Does the project involve new or significantly changed handling of a considerable amount of personal data/special categories of personal data and/or business sensitive data about each individual in a database? | Yes, a minimum dataset would be held in a new clinical system. |
| 1.8 | Data | Does the project involve new or significantly change handling of personal data/special categories of personal data about a large number of individuals? | Yes |
| 1.9 | Data | Does the project involve new or significantly changed consolidation, inter-linking, cross referencing or matching of personal data/special categories of personal data and/or business sensitive data from multiple sources who have not previously had routine access to it? | Yes |
| 1.10 | Data | Will the personal data be processed out of the U.K? | No |
| 1.11 | Exemptions and Exceptions | Does the project relate to data processing which is in any way exempt from legislative privacy protections? | No |
| 1.12 | Exemptions and Exceptions | Does the project’s justification include significant contributions to public security and measures? | No |
| 1.13 | Exemptions and Exceptions | Does the project involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable privacy regulation? | No |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Step 2: Identify the need for a DPIA** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **2.1** | **Is this a new or changed use of personal data/special categories of personal data and/or business sensitive data that is already processed/shared?** | | | | | | | | | | | | | | | | | | | | New/Changed | | | | | |
| Yes | | | | | |
| **2.2** | **What data will be processed/shared/viewed?**  Data to be shared will be determined by source organisations and system design. Yes. Clinician recipients view Patient Confidential Information (PCI) held on a shared EMIS application using an online viewer.  Primary Care (EMIS Web clinical system) controllers can stop specified codes from being viewed by setting rules using the EMIS technical ‘Confidentiality Policy.’ An option can be applied to specific codes on a patient’s record. The national set ‘exclusion code’ list can either be opted in or out of at point of setting-up the EMIS to EMIS sharing (see Schedule 3: GP Summary Exclusion Code List). Note, Primary Care cannot select specific codes to add/remove from this list, it’s an ‘all or nothing’ choice. | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Personal Data**  **Administration data** | | | | | | | | | | | | | | | | | | | | | | | | | |
| Forename | | **X** | | Surname | | | **X** | | | Date of Birth | | | **X** | | | | Age | | | | | **X** | Gender | **X** |  |
| Address | | **X** | | Postal address | | | **X** | | | Employment records | | |  | | | | Email address | | | | | **X** | Postcode | **X** |  |
| Other unique identifier  (*please specify*) | | | | Telephone number | | | **X** | | | Driving licence number | | | **X** | | | | NHS No | | | | | **X** | Hospital ID no | **X** |  |
| Other data *(Please state):* | | | | | | | *N/A* | | | | | | | | | | | | | | | | | | |
| **Special Categories of Personal Data** | | | | | | | | | | | | | | | | | | | | | | | | | |
| Racial or ethnic origin | | | | | | | | **X** | | | Political opinion | | | | | N/A | | | Religious or philosophical beliefs | | | | | **X** | |
| Trade Union membership | | | | | | | | **N/A** | | | Physical or mental health or condition | | | | | | | | | | | | | **X** | |
| Sexual life or sexual orientation | | | | | **X** | | Social service records | | | | | | | X | | | | Child protection records | | | | | | **X** | |
| Sickness forms | **X** | | Housing records | | | | **X** | | Tax, benefit or pension records | | | | | | | | | **N/A** | | | Adoption records | | | **X** | |
| DNA profile | **X** | | Fingerprints | | | |  | | Biometrics | | | **X** | | | Genetic data | | | | | | | | | **X** | |
| Proceedings for any offence committed or alleged, or criminal offence record | | | | | | | | | | | | | | | | | | | | | | | | **X** | |
| `Other data *(Please state):* | | | | | |  | | | | | | | | | | | | | | | | | |  | |
| Will the dataset include clinical data? (please include):  Full coded record, associated free text entries, medications | | | | | | | | | | | | | | | | | | | | | | | **Yes or No** | | |
| Yes | | |
| Will the dataset include financial data? | | | | | | | | | | | | | | | | | | | | | | | **N/A** | | |
| **Description of other data processed/shared/viewed?** | | | | | | | | | | | | | | | | | | | | | | | | | |
| Medical Letters such as test results and other documents via the integrated Docman share app viewer | | | | | | | | | | | | | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **2.3** | **Business sensitive data** | | | | | | |
| Would any of this project decisions impact the Data Controller(s): | One or more business function | | | **Yes/No** | | |
| Yes, individual GP Practices’ online consultations. | | |
| Cohort of data subjects | | | Potentially all patients. | | |
| **Description of other (identifiable or aggregate) data processed/shared/viewed (if any).** | | | | | | |
| The support of the care of patients through consolidated reporting. This is something that already occurs at all practices such as PHM), Activities (including ARRS services), Medicine management (inc. MHRA alerts) and/or QOF &IIF. | | | | | | |
| **Step 3: Describe the sharing/processing** | | | | | | | |
| **3.1** | **List of organisations/partners involved in sharing or processing personal/special categories personal data?** *If yes, list below* | | | | | Yes/No |  |
| Yes |  |
| Name (Controller or Processor) | | Information Commissioner Office registration no | Completed and compliant with the IG Toolkit or [Data Security and Protection (DSP) Toolkit](https://www.dsptoolkit.nhs.uk/) | | |  |
|  | Yes / No | | |  |
| Oaklands Health Centre (C) (lead practice) | | Z7252297 | Yes | | |  |
| Church Road Practice - The Surgery, Lyminge (C) | | Z2193471 | Yes | | |  |
| Harbour Medical Practice (C) | | ZA887309 | Yes | | |  |
| Hawkinge & Elham Valley Surgery (C) | | Z7162265 | Yes | | |  |
|  | New Lyminge Surgery (C) | | Z6288438 | Yes | | |  |
|  | Sun Lane Surgery (C) | | Z8817515 | Yes | | |  |
|  | White House Surgery (C) | | Z6279380 | Yes | | |  |
|  | EMIS Group Plc (P) | | Z2670786 | Yes | | |  |
|  | eConsult Health Ltd (P) | | Z2881782 | Yes | | |  |
| **3.2** | **If you have answered ‘yes’ to 3.1 is there an existing ‘Data Processing Contract’ or ‘Data Sharing Agreement’ between the Parties including with Processor(s) where applicable**  The processing will be partly performed on our behalf by   * EMIS Group Ltd. who provides the electronic patient record solution (clinical system) to the PCN hub**.** EMIS Group Ltd is primarily a UK based business but from time-to-time personal data may need to be transferred outside of the European Economic Area – where this is the case then we will ensure that we have the necessary safeguards in place including prior permissions from us per our contract with EMIS. * eConsult Health Ltd., who provides our online consultation tool. | | | | | Yes/No |  |
| Yes |  |
| **3.3.** | **Has a data flow mapping exercise been undertaken?**  *If yes, please provide a copy, if no, please undertake* | | | | | Yes, See illustration at appendix A |  |
| **3.4** | **Does the project involve employing contractors external to the organisation who would have access to personal or special categories of personal data?**  *If yes, provide a copy of the confidentiality agreement or contract?* | | | | | Yes/No |  |
| Potentially, when this occurs this DPIA will be updated. |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **3.5** | **Describe in as much detail why this information is being processed/shared/viewed?**  *(For example, Direct Patient Care, Statistical, Financial, Public Health Analysis, Evaluation. See NHS Confidentiality Code of Practice Annex C for examples of use)* | | | | | | | | | | | | |
| The purpose of this operating model is to deliver direct patient care under the GMS primary healthcare contract. | | | | | | | | | | | | |
| **3.6** | Will any other stakeholder(s) (whether internal or external) need to be consulted about the proposed processing (e.g., NHS England, Public Health England, NHS Digital, the Office for National Statistics)? And the Outcome(s) of consultation? | | | | | | | | | | | | |
|  | NHS England Southeast Region Primary Care Transformation Programme who has commissioned this pilot work. | | | | | | | | | | | | |
| **Step 4: Assess necessity and proportionality** | | | | | | | | | | | | | |
| **4.1** | **Lawfulness for Processing/sharing personal data/special categories of personal data GDPR 2016 and DPA 2018?**  *In order for the sharing of the personal, and special categories of personal data to comply with* [*GDPR Article 5*](https://gdpr-info.eu/art-5-gdpr/) *and* [*DPA Section 86*](http://www.legislation.gov.uk/ukpga/2018/12/part/4/chapter/2/crossheading/the-data-protection-principles/enacted)*, (principles of data protection) it must be fair, lawful and transparent, and must meet at least one of the* [*Article 6*](https://gdpr-info.eu/art-6-gdpr/) *conditions as well as* [*Article 9*](https://gdpr-info.eu/art-9-gdpr/) *(in the case of special categories of personal data).* [*Article 22*](https://gdpr-info.eu/art-22-gdpr/) *condition must also be met where special categories of personal data are processed using automated individual decision-making, including profiling.* | | | | | | | | | | | | |
|  | |  |  | | --- | --- | | **Conditions relied on under GDPR Article 6** | **Why the conditions are met** | | [Article 6(1) (e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.](https://gdpr-info.eu/art-6-gdpr/) | Access to the information is to provide direct care | | **Conditions relied on under GDPR Article 9** | **Why the conditions are met** | | [Article 9 (2)(h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards](https://gdpr-info.eu/art-9-gdpr/)**.** | Access to the information is to provide direct care | | **Conditions relied on under DPA Section 8** | **Why the conditions are met** | | The lawfulness of sharing/processing of Shared Personal Data set out in Article 6(1) (e) of the GDPR (as above) is also permitted under [Section 8 (d) of DPA 2018:](http://www.legislation.gov.uk/ukpga/2018/12/section/8/enacted)  Processing is necessary for the exercise of statutory functions. | Access to the information is to provide direct care | | **Conditions relied on under DPA Section 10** | **Why the conditions are met** | | The lawfulness of sharing/processing Shared Personal Data set out in [Article 9 (2) (h)](https://gdpr-info.eu/art-9-gdpr/) of the GDPR (as above) is permitted under [DPA Section 10 (health and social care purposes)](http://www.legislation.gov.uk/ukpga/2018/12/section/10/enacted) | Provision of health care. | | **Conditions relied upon for obligation of professional secrecy** | **Why the conditions are met** | | For the purposes of Article 9(2) (h) of the GDPR, the circumstances in which the processing of Shared Personal Data is carried out is subject to the conditions and safeguards referred to in [Article 9(3)](https://gdpr-info.eu/art-9-gdpr/) of the GDPR (obligation of professional secrecy). Therefore, in accordance with [DPA Section 11(1)](http://www.legislation.gov.uk/ukpga/2018/12/section/11/enacted), these include circumstances in which it is carried out –   1. by or under the responsibility of a health professional or a social work professional, or   by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law. | Carried out by a health professional | | **Common law duty of confidentiality** | Implied whilst shared during the provision of direct care. | | | | | | | | | | | | | |
| **4.2** | **Will the information be processed/shared electronically, on paper or both?** | | | Electronic | | | | | | | | X | |
| Paper | | | | | | | |  | |
| **4.3** | **How will you ensure data quality and data minimisation?** | | | | | | | | | | | | |
| **Data Quality**  Data quality responsibilities fall to individual practices managing patients’ record to check that the information being shared is accurate and up to date. EMIS product has the mandatory DSB0129 Clinical Safety Case, and that the implementation is being handed over as per DSB0160. There are no additional data quality checks undertaken for data viewed at the hub. Protocols are in place within the practice on best practice with regard Data quality when completing patients’ records. However, there may be inadvertent inaccuracies in historical data which the practice will have a duty to address and possibly rectify if requested.  **Data Minimisation and proportionality**  Data will be shared between the Folkestone, Hythe and Rural PCN practices and the PCN hub via EMIS-to-EMIS clinical system sharing to include view only access (non-editable). This will apply to the full medical records, coded entries, free text entries, medication, and all attachments.  Attachments on a patient’s record may have been created in a number of ways:   * Filed directly to a patient record from a document received into EMIS electronically; * As a result of a referral being created within EMIS; * Manually attached via EMIS; and/or * Attached to the patient record using Docman   In the last of these examples, when an attachment is added to the EMIS record using the Docman system EMIS assumes that you will be using Docman to open the attachment from the EMIS record.  This has meant purchasing a Docman Share configuration that will allow the PCN to view these attachments within the PCN EMIS but through an integrated Docman viewer.  The viewer has full integration within PCN EMIS, is single sign-on and patient context aware.  It is only configured between FHR PCN practices and PCN EMIS hub.  So, these attachments are not made available outside of FHR PCN via Docman Share configuration.  Docman viewer sharing will be enabled until a suitable technical solution to integrate Docman viewing letters into EMIS is technically effected into the clinical system. | | | | | | | | | | | | | |
| **4.4** | **How will personal data be collected in each case?** *For example, from data subjects directly or from 3rd parties. If 3rd parties, identify them.* | | | | | | | | | |  | | |
|  | Directly via their practices’ EMIS clinical system and sometimes from patients during consultation. | | | | | | | | | |  | | |
| **4.5** | **If the project requires processing of special categories of personal data, do the Controller and its representative have in place a Record of Processing Activity?** *This can also be the Data flow map.*  *In order to demonstrate compliance with GDPR Art. 30 and DPA Section 61, the controller or processor should maintain Records of Processing Activities (RoPA) under its responsibility. The RoPA shall contain the name and contact details of the controller and, where applicable, the joint controller, the controller’s representative and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the categories of personal data; and the categories of recipients to whom the personal data have been or will be disclosed.* | | | | | | | | | | Yes, each Practice member of the PCN has one that includes the data flow to/from PCN. | | |
| **4.6** | **If the project requires processing of special categories of personal data, do the Controller and its representative have in place an “Appropriate Policy Document” that explains the "safeguards" in place for processing the special categories of personal data? And also, informing individuals about the proposed use of their personal or special categories of personal data?**  *Part 1 of Schedule 1 (4) of DPA 2018 requires a Controller and Processor to have an Appropriate Policy Document in place for processing relating to employment, social security and social protection, Health or social care and public health purposes. The Policy should explain controller/processor’s procedures for securing compliance with the principles relating to processing of special categories of personal data; explain the controller/processor’s*  *For example, do the organisations/partners listed in section 3.1 have updated Privacy Notice available to patients on their websites and as regards the retention and erasure of special categories of personal data, and giving an indication of how long such data is likely to be retained.* | | | | | | | | | | Yes, each practice has a patient facing privacy notice which is updated with this PCN level processing and appropriate internal IG policies | | |
| **4.7** | **How will we ensure the accuracy of the personal data (including their rectification or erasure where necessary)?** **How will we monitor the quantity of the personal data?** | | | | | | | | | |  | | |
| Identifiable personal and health related data will be recorded on either EMIS clinical services by a member of the PCN’s team who should ensure that checks take place to ensure the accuracy of the information provided.  Any identifiable personal data held within EMIS should be confirmed at the point of contact and updated on the National Spine and/or local systems where necessary.  Local practice policies regarding IT systems.  All Practices that form the Folkestone, Hythe and Rural PCN have in place a suite of IG policies and processes in compliance with the NHS DSPT.  A Joint Controllers’ Data Sharing Agreement has been worked up in order to agree roles and responsibilities in managing data that is hosted within the PCN EMIS Clinical Service.  All Practices that form the PCN have in place processes for patients to exercise their rights. Details of how to contact individual Practice’s to exercise their rights are detailed in individual Privacy Notices.  Whilst Patients may use eConsult to contact the PCN they may request a consultation by their own Practice and at that point they would exercise their “right to object” to processing by another Practice within the PCN.  At stated in the project summary, there are technical limitations to the process of integrating the PCN hub configured EMIS clinical system with each of the 7 GP practices EMIS systems to automatically recognise/synch all patients’ records. This means that there will be a manual mass upload/pre-registration of all patients at all 7 practices onto the PCN hub’s EMIS clinical system. EMIS Group Plc providing the clinical system solutions have been commissioned to do this mass upload and to periodically update any new registrations (quarterly). This is manually done owing to the limitation of technology at this time. This is in compliance with the provisions of article 5 (1) (f) and 32, recital 39 and 83 of the UK GDPR that recognises that data processing will be by means of security measures that are within the capacity of available technologies at the time (technology limitations). There is ongoing discussion between NHS England and EMIS to enable this integration functionality in due course.  For the exceptional patients that could not form part of the mass pre-registration, these are estimated to be of low numbers and within capacity to be individually registered when they present. | | | | | | | | | |  | | |
| **4.8** | **Are arrangements in place for recognising and responding to Subject Access Requests (SARs)?** | | | | | | | | | | | | |
| As joint data controllers, each local GP Practice within the PCN will be responsible for fulfilling their own requests for copies of personal data. From completing this DPIA, it has also been determined that the (FHR) PCN would be data controllers in its right owing to the data they would be processing and making decisions over at a central level which would be held by them indefinitely similarly to how GP Practices or core NHS provider currently hold data. However, under the current model of lead practice as PCNs are not typically legal entities, this places an additional responsibility on the lead practice in terms of their data protection responsibilities as they would be representing the PCN as well.  Under the FHR PCN lead practice model, Oaklands health centre (as the lead practice) will handle any SAR made specifically to the FHR PCN where applicable. However, SARs requests to the PCN specifically is expected to be low (if any) as this is mitigated by the hub project itself, as all data processed at PCN hub level will be flowed back to each practice who will release it as part of normal SAR requests to the practice. | | | | | | | | | | | | |
| **4.10** | **Will the processing of data include automated individual decision-making, including profiling?**  *If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject* | | | | | | | | | No | | | |
|  | | | | | | | | | | | | | |
| **4.11** | **Will individuals be asked for consent for their information to be processed/shared?**  *If no, list the reason for not gaining consent e.g., relying on other lawful basis, consent is implied where it is informed.* | | | | | | | | | No | | | |
|  | Relying on other lawful bases for providing direct care | | | | | | | | | | | | |
| **4.12** | **As part of this work is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier? If so, please complete an Information Security (IS) risk assessment.** | | | Yes, EMIS utilises cloud technology. Their information security framework has been risk assessed and they have the following subsisting certifications:   * Cyber Essentials Plus * ISO 27001:2013 * ISO 22301:2019 * ISO 9001:2015 * ISO 20000:2018 | | | | | | | | | |
| **4.13** | **Where and how the data will be stored**  *Examples of Storage include bespoke system (e.g., EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc.* | | | | | | | | | | | | |
| There are two repositories utilised for the hosting of patient records:   * EMIS Web clinical system at the practice where the patient is registered. * EMIS Clinical Service clinical system that is used across the Folkestone, Hythe and Rural PCN.   (EMIS Enterprise Search and Reporting unit). | | | | | | | | | | | | |
| **4.14** | **Data Retention Period**  *How long will the data be kept?* | | | | | | | | | | | | |
| All records will be kept and erased/destroyed in compliance with the NHS Record Management Code of Practice 2021  Sessional viewing only. Data not retained – read only.  Information will be retained in the core providers system. Any information accessed by the hub’s will be on a view only basis. However, recorded data during hub sessions will be able to go back for inclusion into the GP systems as well. | | | | | | | | | | | | |
| **4.15** | **Will this information be shared/processed outside the organisations listed above in question 3?**  *If yes, describe who and why:* | | | | | | | | | | | Yes/No | |
| No | |
| Not directly from the PCN level. However, as the consultations are written back to the patient’s GP record they will be fed into their sharing/processing arrangements that are already in place. | | | | | | | | | | |  | |
| **Step 5: Information Security Process** | | | | | | | | | | | | | |
| **5.1** | **Is there an ability to audit access to the information?** | | | | | | | | | | | Yes/No | |
| Yes | |
| There is a full end to end audit in place within EMIS Web and the EMIS Clinical Service. This audit can be used to see activity data in terms of record access and actions taken upon patient records. The audit trails can be run at a practice level, or within the EMIS Clinical Service. | | | | | | | | | | |
| **5.2** | **How will access to information be controlled?** | | | | | | | | | | | | |
| Only access by people involved in the patients’ care including clinical and non-clinical staff.  EMIS Web clinical system is hosted in Leeds Information is stored in EMIS Datacentres which have the appropriate technical and organisational measures in place to protect against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data;   * IGSoC v11 compliant * Registered to ISO 20000, ISO 27001 and ISO 14001 * Subject to 6 monthly audits for ISO27001 compliance, by BSI (UKAS 0003)   Beyond EMIS Web clinical system, if we are to use another non-EMIS clinical system, consultation documents viewed on EMIS can be printed or right click and saved into local system within appropriate controls. | | | | | | | | | | | | |
| **5.3** | **What roles will have access to the information?** (list individuals or staff groups) | | | | | | | | | | | | |
| Clinical and administrative staff employed by the 7 GP practices that sit within Folkestone, Hythe and Rural PCN along with clinicians and administrators contacted by Folkestone, Hythe and Rural PCN GP practices to deliver healthcare services under the ARRS scheme (for example First Contact Physiotherapy, Occupational Therapy, Mental Health Practitioner).  Where the data sharing has been activated for the PCN hub EMIS clinical system, full records can be viewed by PCN hub staff who have been assigned the correct Role Based Access Control (RBAC) access. The intended use is in clinical settings to provide health professionals with access to a patient's Primary Care Record for the purpose of direct care delivery. RBAC roles and permissions are relative to Smartcard the clinician holds. RBAC roles are assigned for specific purposes to support direct care. | | | | | | | | | | | | | |
| **5.4** | **What security and audit measures have been implemented to secure access to and limit use of personal data/special categories of personal data and/or business sensitive data?** | | | | | | | | | | | | |
| Username and password | X | Smartcard | | **X** | key to locked filing cabinet/room | | | | | | |  |
| Secure 1x Token Access |  | Restricted access to Network Files | | | | | | | | | |  |
| Other: *Provide a Description Below*: | | | | | | | | | | | | |
| Access to the EMIS Web clinical system data is granted through local RBAC policy and subject to practice controls.  Each GP practice must:   * Annually complete and adhere to the Data Security and Protection Toolkit (formerly the IG Toolkit) * Ensure all staff complete mandatory annual information governance training. * Maintain a suite of information governance policies (e.g., confidentiality, security, and data protection) in place that their staff must adhere to, * Ensure all staff sign-up to Confidentiality Code of Conduct.   The system is secure as it meets the GP Systems of Choice (GPSoC) framework and requirements  Technical security is provided by EMIS utilising the HSCN connection and requiring RBAC Registration Authority SmartCards and two- factor authentication.  All EMIS systems that have been mentioned as being in scope for this project all operate over an HSCN secure connection. Accounts are role based with password protection and associated with an NHS.net email account. | | | | | | | | | | | | |
| **5.5** | **Is there a documented System Level Security Policy (SLSP) and/or for this project? If yes, please embed a copy below:**  *SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.* | | | | | | | Yes/No | | | | | |
| Yes, A policy for on/off boarding staff to PCN EMIS system esp as under current model, staff would be technically employed by member GP practices for the PCN. | | | | | |
| **5.6** | **Are there Business Continuity Plans (BCP) and Disaster Recovery Protocol for the proposed/existing system or process? How will the personal data be restored in a timely manner in the event of a physical or technical incident?**  *Please explain and give reference to such plan and protocol* | | | | | | | Yes | | | | | |
| Yes | | | | | |
| Patient interactions will be documented one both the PCN EMIS clinical and on each practice’s electronic patient records, they will therefore act as a backup for one another should there be a physical or technical incident that affects the data. Also, the overarching Contract with EMIS is held nationally and covers Business Continuity Planning. Failover is undertaken by EMIS utilising a number of failover techniques and processes which involve locations, hardware, software and processes. | | | | | | | | | | | | | |
| **5.7** | **Is Mandatory Staff Training in place for the following?** | | | | | | Yes/No | | Dates | | | | |
| * Data Collection: | | | | | | Yes | | Annually | | | | |
| * Use of the System or Service: | | | | | | Yes | | Annually | | | | |
| * Information Governance: | | | | | | Yes | | Annually | | | | |
| **5.8** | **Are there any new or additional reporting requirements for this project?** | | | | | |  | | | | | | |
| * What roles will be able to run reports? | | | | | | | | | | | | |
| EMIS Web clinical system will allow system access audit reports to be available to the defined RBAC role, generally practice managers and those in the RBAC Privacy Officer role for the practice employing the clinicians, but can be more than one person, e.g., IT/IG lead, Practice Manager or Lead Clinician | | | | | | | | | | | | |
| * What roles will receive the report or where will it be published? | | | | | | | | | | | | |
| Only those who have the defined RBAC role to run audit rights within each provider organisation will receive audit reports.  The organisations contributing to the shared record will be able to request audit reports on who accessed records and reports on who accessed a given patient's records. | | | | | | | | | | | | |
| * Will the reports be in person-identifiable, pseudonymised or anonymised format? | | | | | | | | | | | | |
| Person identifiable.  Privacy reports can be configured by the person running the report. There are a wide range of fields that can be included for each record accessed, e.g., NHS number, Date and time of Access, Username, Designation, Reason for viewing, Provider name etc. | | | | | | | | | | | | |
| * Will the reports be in business sensitive or redacted format (removing anything which is sensitive) format? | | | | | | | | | | | | |
| Business sensitive | | | | | | | | | | | | |
| **5.9** | **Will the data be linked with any other data collections?**  Any data that resides within the EMIS Clinical Service will also be fed through to the PCN’s EMIS Enterprise instance, which is used to pull reports. These reports are used for improving patient care and service delivery. | | | | | | | | | | | **Yes/No** | |
| Yes | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Step 6: Identify and Assess Risks (Review and Risk Matrix)** | | | | | | | | | | | | |
| Are there any risks to the **Confidentiality** of personal data? *Confidentiality is defined as unauthorised disclosure of, or access to, personal data.*  Row-level data downloaded to a portable storage device or computer for local processing (e.g., spreadsheet). Individuals motivated to act beyond their authorisation particularly staff who work at both Practice and PCN levels. This may be out of enthusiasm, with malicious intent or for personal gain.  Yes - There is a risk of unauthorised disclosure of, or access to, personal data while transporting, storing, or accessing personal data. | | | | | | | | | | | | |
| Are there any risks to the **Integrity** of personal data? *Integrity is defined as unauthorised or accidental alteration of personal data.*  Yes - The risk would be the same, or similar, as is accepted within any of the constituent practices.  Yes – There is a risk to the integrity of personal data | | | | | | | | | | | | |
| Are there any risks to the **Availability** of personal data? *Availability is defined as unauthorised or accidental loss of access to, or destruction of personal data.*  Yes – There is a risk of unauthorised or accidental loss of access to, or destruction of personal data  Yes - Unavailability of Assets or services: processing is delayed.  Yes - Excessive data processing owing to practice-to-practice consultation write back (CWB) being triggered.  Yes - owing to CWB not working leading to patient’s data not being fed back to their GP Practice as only an EMIS consultation will trigger a CWB. For example, the patient is not registered with a constituent practice or there is a technical outage of service.  Yes – processing beyond defined retention period. | | | | | | | | | | | | |
| *Are there any known or immediate technical / IT / Information Security / Cyber Security concerns?*  Yes – the consultation write back (CWB) of data to their GP Practices (practice to practice CWB issue, editing consultation issue, limitation of what can trigger a CWB).  Yes – mass upload of all patients’ data in all 7 practices to the PCN EMIS clinical systems.  Yes – maintaining of the PCN EMIS clinical system alongside the (lead) practice’s own EMIS clinical system leading to being data controller for 2 separate regimes. | | | | | | | | | | | | |
| An additional responsibility on the lead practice in terms of their data protection responsibilities as they would be representing the PCN as well.  Non-compliance with article 28 of GDPR to have an appropriate DPA in place with data processors (EMIS, e-consult). | | | | | | | | | | | | |
| **Step 7: Identify Measures to reduce risk** | | | | | | | | | | | | |
| **If the answer is “Yes” to any questions in step 6, how are these to be reduced or mitigated?**  **See risk description below.** | | | | | | | | | | | | |
| **Once the mitigations are implemented, how would you score any remaining risk in the following Risk Assessment? If you consider that there are no remaining risks give a value of 1 for both Likelihood and Severity.** | | | | | | | | | | | | |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | **Likelihood** *(please tick)* | | | **x** | **Severity** *(please tick)* | | | **=** | | **1** |  | Rare |  | **1** |  | Negligible |  | | **2** |  | Unlikely | **2** |  | Minor |  | | **3** |  | Possible | **3** |  | Moderate |  | | **4** |  | Likely | **4** |  | Major |  | | **5** |  | Almost certain | **5** |  | Catastrophic |  | | | | | | | | | | | | | |
| LIKELIHOOD | | IMPACT / CONSEQUENCES | | | | | | | | | |  |
| NEGLIGIBLE | | MINOR | MODERATE | | MAJOR | | | CATASTROPHIC | |  |
| 1 | | 2 | 3 | | 4 | | | 5 | |  |
| 1 (rare) | | **L** | | **L** | **M** | | **H** | | | **H** | |  |
| 2 (unlikely) | | **L** | | **L** | **M** | | **H** | | | **E** | |  |
| 3 (possible) | | **L** | | **M** | **H** | | **E** | | | **E** | |  |
| 4 (likely) | | **M** | | **M** | **H** | | **E** | | | **E** | |  |
| 5 (almost certain) | | **M** | | **H** | **E** | | **E** | | | **E** | |  |
| **Step 8a: Data Protection Risks**  **List any identified risks to Data Protection and personal information of which the project is currently aware.**  **Risks should also be included on the project risk register.** | | | | | | | | | | | | |
| **Risk Description**  **(to individuals, to the CCG or to wider compliance)** | **Current Impact (after mitigation)** | **Current Likelihood (after mitigation)** | **Risk Score (I x L) (after mitigation)** | **Proposed Risk solution (Mitigation)** | | | | **Is the risk reduced, transferred or accepted? Please specify.** | | **Evaluation: is the final impact on individuals after implementing each solution a justified, compliant, and proportionate response to the aims of the project?** | | |
| An additional responsibility on the lead practice (Oaklands Health Centre) in terms of their data protection responsibilities as they would be representing the PCN as well. | 2 | 3 | 6 | A robust Joint Controller’s Data Sharing Agreement has been created for all members of the FHR PCN. This incorporates the clause that any risk borne by the lead practice on behalf of the PCN is borne and shared equally by all members. | | | | Reduced and accepted | | Yes, it is.  The PCN hub has been set up to operate to applicable statutory requirements which include the lead practice model (i.e., under the NHS PCN Agreement) | | |
| The EMIS Clinical Service requires that a new ‘Community’ registration type patient record is created in order for the PCN Hub user to record a consultation.  This manual registration process in the EMIS Clinical Service is called ‘Patient Trace’. There is a risk that the wrong patient is traced into the system. | 3 | 2 | 6 | The trace procedure queries the local database, if the patient is not found the practice databases are queried if the patient is not found a prompt to register the patient via PDS is presented. Staff are trained to:  a) check and reconcile patient trace returns against details of the patient that they wish to register  b) investigate further if prompted by the system to register patient via PDS as under usual circumstances the system should find the patient either in its own database, or one of the practice databases.  The system provides fully auditable tools to amend any incorrectly registered patient and take appropriate action on the corresponding GP practice record if applicable. | | | | Reduced and accepted | | Yes, it is.  As a future mitigation, the PCN has worked with EMIS on an enhancement that sees the demographics included with an online consultation, and required to trace the patient, automatically pulled into the patient trace screen as opposed to being manually entered. This reduces the risk to transcribing errors by users. Timescales for the rollout of this functionality TBC. | | |
| Availability/IS (clinical) risk owing to (excessive data processing) practice to practice consultation write back (CWB) being triggered. | 3 | 2 | 6 | By default, EMIS configure Consultation Write Back functionality within a ‘many to many’ technical data sharing agreement. This leads to consultations not being sent back from just hub to practice, but also practice to practice where a patient is registered within a constituent practice system with an additional registration type such as ‘temporary’, and a full GP registration in another constituent practice clinical system.  The issue of ‘practice to practice’ write back was picked up at an early stage of the pilot and addressed through the implementation of a series of ‘one to one’ technical data sharing agreements. This mitigates the risk of ‘practice to practice’ write back entirely. | | | | Reduced and accepted | | Yes, it is.  EMIS is due to release an amendment to the way in which the technical sharing agreements for Consultation Write Back work. In the interim, EMIS will accept requests for one-to-one technical sharing agreements for consultation write back from other PCNs upon request.  A DCB160 has been written for the project. | | |
| Availability/IS (clinical) risk owing to CWB not being triggered leading to patient’s data not being fed back to their GP Practice as only an EMIS consultation will trigger a CWB. For example, the patient is not registered with a constituent practice or there is a technical outage of service. | 3 | 2 | 6 | This type of issue is mitigated through the use of:  - Staff training, to ensure that staff are able to recognise a failed CWB or where an entry will not trigger a CWB along with the significance of this and required follow-up actions. E.g., constituent practice system access is available to all PCN staff to ensure that any entries not sent back via consultation write back can be manually added to the patient’s GP record.  - System audit, using the EMIS Clinical Service reporting capabilities to search for record entries that do not have a 'Sent' status.  - Full bi-directional care record sharing, allowing a practice to view the PCN Hub record in full, regardless of any CWB entries that have failed. | | | | Reduced and accepted | | Yes, it is.  **N.B**: During the pilot EMIS advised that there may be a future enhancement that allows failed CWB entries to be re-sent.  A DCB160 has been completed. | | |
| Availability/IS risk owing to incomplete information being written back to the Practice i.e., because any edits made to an original consultation already written back will not be sent to the practice. | 3 | 2 | 6 | Where an edit needs to be reflected in the GP practice system this would need to be manually completed by logging into the GP system that CWB has written back to. Furthermore, there was an enhancement added to the CWB functionality by EMIS that altered a user when they were attempting to edit a consultation for which CWB had already triggered.  PCN Hub staff will be trained that this is how the functionality works in order to minimise the likelihood of a hub consultation needing to be edited. | | | | Reduced and accepted | | Yes, it is. A DCB160 has been completed. | | |
| Non-compliance with the UK GDPR principle of proportionality where patients’ data is being held simultaneously and with no retention period on both their GP system once written back and on the hub. | 1 | 4 | 4 | As it stands, the PCN EMIS record would not be deleted as it would not be manageable to keep registering and then closing the patient records in the PCN EMIS as a going concern. It would be a significant task to delete these contacts in the hub. | | | | Reduced and accepted | | Yes, it is  In essence, the PCN hub is seen as another NHS provider capable of owning and managing patients’ data. | | |
| Non-compliance with article 28 of GDPR to have an appropriate DPA in place with data processors (EMIS) | 3 | 2 | 6 | Appropriate data processing clauses in place between the PCN and the identified data processors i.e., EMIS as stated within the SLA and T&Cs. | | | | Reduced and accepted | | DPA terms are included across EMIS Ts&Cs and SLA. Additionally, a standalone DPA is being worked on. | | |
| Breach of confidentiality – unlawful access to record (by staff) | 2 | 2 | 4 | Role Based Access  Training for all staff  Employment contracts and Code of Confidentiality  Professional registration  Audit trail & disciplinary action – deterrent.  Controls are in place to prevent data from being downloaded or ‘screen-scraped’, such as VPN remote access, or use of TTP proprietary analysis tools | | | | Reduced and accepted | |  | | |
| Loss of data (temporary or permanent), due to technical / security failure | 3 | 2 | 6 | Business Continuity Plan  Network security & Data Centre security  Pen Test and Vulnerability Scan | | | | Reduced and accepted | |  | | |
| Unlawful processing or sharing of data | 3 | 2 | 6 | Governance processes including DPIA, Data Sharing Framework.  Periodic review of IG documents and processes | | | | Reduced and accepted | |  | | |
| Patients’ rights and freedoms are compromised | 3 | 1 | 3 | GP Practice level PN already references data flow to PCN level.  Processes in place for patients to exercise their rights at GP level. | | | | Reduced and accepted | | If the PCN transitions to its own entity, it can maintain a patients’ PN at PCN level. | | |
| Governance- Data Control  Lack of clarity over apportionment of data control responsibilities and accountabilities resulting in poor transparency and uncertainty over liabilities, risk ownership, indemnities | 3 | 1 | 3 | Project is under PCN Joint Control and a JC’s DSA in place to describe parties’ rights and responsibilities.  Operating procedures ensure responsibility and accountability by design. | | | | Reduced and accepted. | |  | | |
| Governance – Unlawful processing  An ‘instruction to process’ issued directly by one of the PCN members to a Trusted Third-Party (TTP) data processor without the prior knowledge or agreement of other controllers | 3 | 1 | 3 | The Joint Control arrangement has robust audit trails to ensure all controllers act within their responsibilities.  TTPs are held to contracts, which if found in breach can be terminated.  The PCN central administrative office authorise users and managing access rights for roles and permissions. | | | | Reduced and accepted | |  | | |
| Governance – project or mission creep  New projects or services that extend processing activities beyond its mandate or stated purpose(s). | 3 | 1 | 3 | Each new service will be subject to mandatory review of this DPIA or draft of a purpose specific DPIA | | | | Reduced and accepted | |  | | |
| Governance – reputational damage  A reported loss or breach incident, or poor data protection practices questioned by press attention | 3 | 2 | 6 | To agree a set review date for the IG of this pilot project and potential transition into a full live service | | | | Reduced and accepted | | Recommended review date of this DPIA is 6months from date of completion. | | |
| Individual rights and freedoms - Objections and Opt-outs  Individuals have the right to object the further use of their health data for analytics or research purposes. | 2 | 2 | 4 | Processes are in place to restrict or prevent processing where an individual objects and model GP Practice members’ privacy notices must explain in plain English how patients can exercise their rights. | | | | Reduced and accepted | |  | | |
| **Step 8b: Actions to be taken** | | | | | | | | | | | | |
| **Actions to be taken** | | | | | | | | **Date of Completion** | | | **Action Owner** | |
| Joint Controllers’ Data Sharing Agreement Framework to be drafted | | | | | | | | Completed | | | LA | |
| Member GP Practices should update their privacy notice with the data flow to the PCN (clinical system). If/when the PCN becomes a legal entity, to create its own privacy notice. | | | | | | | | Completed | | | LA | |
| A record of processing activities (ROPA) for the project to be developed and maintained for PCN level data processing. | | | | | | | | Completed | | | LA | |
| An information asset register to be maintained at PCN level, separate from the lead practice (can be included in the ROPA). | | | | | | | | Completed | | | LA | |
| **Step 9: Sign off and record outcomes** | | | | | | | | | | | | |
| **Item** | | **Name/date** | | | | | | | **Notes** | | | |
| Measures approved by: | |  | | | | | | | Integrate actions back into project plan, with date and responsibility for completion | | | |
| Residual risks approved by: | |  | | | | | | | If accepting any residual high risk, consult the ICO before going ahead | | | |
| DPO advice provided: | | Latifa Aina  13/07/2023 | | | | | | | DPO should advise on compliance, step 6 measures and whether processing can proceed | | | |
| **Summary of DPO advice**:   * All attempts have been made to mitigate known risks that have presented from a data protection perspective. And as a pilot scheme, I would recommend a review of this DPIA in 6 months, at the latest in 12 months from the date of completion. * For this project, the PCN maintains its own EMIS clinical system from which data is flowed back to GP practices, potentially making the PCN a data controller. However, the PCN is not a legal entity but uses the lead practice model; and it isn’t possible for the lead practice to be a data controller in 2 separate capacities. Working within the current PCN statutory framework (NHS PCN Agreement), a robust Joint controllers’ data sharing agreement between the members of the PCN has been worked up to equally disburse all risks amongst all members of the PCN, to minimise extra risks to the lead practice. * It has been fed back to NHS E for subsequent contractual review of the PCN framework model to consider compelling PCNs to operate from a flat structure such that PCNs are CQC, ICO and DSPT registered entity on their own providing healthcare, able to act independently; and absorb any legal/contractual risks. | | | | | | | | | | | | |
| **DPO advice accepted or overruled by**: | |  | | | | | | | If overruled, you must explain your reasons | | | |
| **Comments**: | | | | | | | | | | | | |
| **Consultation comments (if applicable)** | | | | | | N/A | | | | | | |
| **Signed by SIRO (Name, date & signature):** | | | | | | **SIRO Comment**: | | | | | | |
| **Signed by Caldicott Guardian (Name, date & signature):** | | | | | | **Caldicott Comment:** | | | | | | |
| **This DPIA will kept under review by:** | |  | | | | | | |  | | | |

**Appendix A:** The Folkestone, Hythe and Rural PCN Hub schematic overview

