# Data Protection Impact Assessment (DPIA)

Please complete all questions with as much detail as possible (liaising with partners/third parties) and then contact the IG Team prior to seeking approval.

**Section 1: System/Project General Details**

|  |  |
| --- | --- |
| **System/project/process (referred to thereafter as ‘project’) title:** | Community MSK Physiotherapy Service |
| **Objective:** | Provision of MSK physiotherapy solutions for non-complex MSK cases, delivered via referral from the GP or via self-referral, in a community setting |
| **Detail:**Why is the new system/change in system required? Is there an approved business case? | The change in the system regarding data relates to the new option to self-refer into the service. This is required in order to 1) remove barriers for individuals wishing to access the community provider of their choice and also (2) to reduce time requirements on GPs (who historically had to refer patients into the system, as the only means of entry). The business case was put before the CoM and CCC for approval.  |
| **Stakeholders/Relationships/Partners:**Please outline the nature of such relationships and the corresponding roles of other organisations. | 10 community MSK physiotherapy providers – clients can contact then directly for MSK services (MSK providers will assess appropriateness and treatment need and liaise with GPs if required (i.e. for ongoing secondary treatment referrals) and consented to. GPs may also refer to the MSK providers, with client agreement. In both cases, with agreement, a closing summary of the treatment will be provided by the MSK providers to the GP. The MSK providers also report on the service to the CCG (IAA), but with non-patient identifiable data – the volume flow information informs payment for the service and targeted updates to the referring GPs. |
| **Other related projects:** | Via request to the GP, this service can refer into other secondary services as required |
| **Project lead:** | Title: | Service lead, carers and communities |
| Department: | Care & Independence team |
| **Information Asset Owner:**All information systems/assets must have an [Information Asset Owner (IAO).](#IAO) IAO’s should normally be a Head of Department/Service. | Title: | Service lead, carers and communities |
| Department: |  Care & Independence team |
| **Information Asset Administrator:**Information systems/assets may have an [Information Asset Administrator (IAA)](#IAA) who reports the IAO. IAA’s are normally System Managers/Project Leads. | Title: | Commissioning Officer |
| Department: | Care & Independence team |

**Section 2: Data Protection Impact Assessment Key Questions**

|  | **Question** | **Response** |
| --- | --- | --- |
| **Data Items** |
|  | **Will the project use identifiable or potentially identifiable data in any way?**If answered ‘No’ then a DPIA is not normally suggested. | [x]  Yes [ ]  NoIf yes, who will this data relate to:[x]  Patient[ ]  Staff[ ]  Other: Click here to enter text. |
|  | **Please state purpose for the processing of the data:**For example, patient care, commissioning, research, audit, evaluation. | MSK providers process/store the information in order to ensure appropriate patient care planning. The GP data is to ensure GPs have a full picture of the health of their clients, and can use this to inform any further actions/referrals. The CCG processing of data (non-patient identifiable) is to inform the use of the service, from what quarters, and satisfaction for evaluation, payment and future service improvements. |
|  | **Please tick the data items that are held in the system****Personal****Special categories** **of personal data** **(sensitive data)** |  [x]  Name [x]  Address [x]  Post Code [x]  Date of Birth [x]  GP Practice [ ]  Date of Death [x]  NHS Number [ ]  NI Number [ ]  Passport Number [x]  Pseudonymised Data [ ]  Online Identifiers (e.g. IP Number, Mobile Device ID)[x]  Health Data [ ]  Trade Union membership[ ]  Political opinions [ ]  Religion[ ]  Racial or Ethnic Origin [ ]  Sex life and sexual orientation[ ]  Biometric Data [ ]  Genetic Data [ ]  Other:  |
|  | **What consultation/checks have been made regarding the adequacy, relevance and necessity for the processing of the data for this project?** | The self-referral form has been researched against other comparable self-referral systems for MSK, and will be passed to the MSK providers for comment before start of service, to ensure information requested is adequate, relevant and necessary. The GP referral form was approved for use with the service 4 years ago and has not changed.  |
|  | **How will the data be kept up to date and checked for accuracy and completeness?** | Clients are referred into the MSK service for a clinically relevant time period, but this is not long. During the treatment, ongoing assessment of the condition occurs, and at treatment end, a summary of the treatment and any further steps is passed to the GP (with client’s consent). Therefore, keeping the data up to date is not really a relevant issue. With self-referral, clients are asked to sign off on the information they provide to ensure it is accurate and complete. With GP referral, any discrepancies in contact information is checked by MSK therapists with the GP and other information is proof checked with the client at appointment.  |
| **Data processing** |
|  | **Will a third party be processing data on the CCG or one of its contractors?** | [x]  Yes [ ]  NoIf no, please go to the Confidentiality section.  |
|  | **Is the third party contract/supplier of the project registered with the Information Commissioner?**This was required until 25 May 2018. | [x]  Yes [ ]  NoRefer to risk assessment – for full detailsOrganisation: All organisations Data Protection Registration Number: refer to risk assessment action 1 – |
|  | **Has the third party supplier completed and published a satisfactory** [**Data Security and Protection Toolkit submission**](https://www.dsptoolkit.nhs.uk/)**?**Please note that the Data Security and Protection Toolkit replaced the IG Toolkit from 1 April 2018. | [x]  Yes [ ]  NoIf yes, please give organisation code and percentage score:Refer to risk assessment for full details. Capital Physio completed toolkit 21.11.19*IG Toolkit Score:*[ ]  Satisfactory [ ]  Not satisfactory[ ]  Satisfactory with Improvement PlanIf satisfactory with an improvement plan, please request a copy of the plan and enclose it with this assessment.If not satisfactory, please explain how the service has been procured:Click here to enter text. |
|  | **Does the third party/supplier contract(s) include all the necessary Information Governance clauses regarding Data Protection and Freedom of Information?**See [Contract and Commissioning Information Governance Assurance](#SupportingDocs) checklist. | [x]  Yes [ ]  NoIs the contract based on or utilise the NHS standard contract?[x]  Yes [ ]  No |
|  | **Will other third parties (not already identified) have access to the data?** Include any external organisations. | [ ]  Yes [x]  NoIf so, for what purpose?Click here to enter text.Please list organisations and by what means of transfer:Click here to enter text. |
| **Confidentiality** |
|  | **Please outline how individuals will be informed and kept informed about how their data will be processed.**A copy of the [privacy notice and/or leaflets](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) must be provided. | The data is used in conjunction with an assessment to explore the healthy condition and create a treatment plan – the patient is involved directly in this. Consent is sought from clients at the beginning to share the medical situation and outcomes of treatment with the GP. |
|  | **Does the project involve the collection of data that may be unclear or intrusive?**Are all data items clearly defined? Is the data collected limited to a specific set of predefined categories? | [ ]  Yes [x]  NoIf yes, please explain:Click here to enter text. |
|  | **Are you relying on individuals (patients/staff) to explicit consent to the processing of personal identifiable or sensitive data?**Please provide copies of any consent documentation that will be used, including patient information leaflets | [ ]  Yes [x]  No (Go to next question)There is assumed consent in regards to self-referral, in that the patient is putting themselves forward and submitting their own data for use in expectation of a service (and this is what the information is processed for). There is also explicit consent in regards to sharing the data and outcomes of treatment with the GP – MSK therapists will obtain this directly via the form and conversation. Where the client is GP referred, the GP will obtain the client’s permission to have their data sent to the MSK provider for use as above. In this case, returning updates from the MSK provider is covered as part of the GP consent at the start.Will the consent cover all proposed processing and sharing/disclosures?[x]  Yes [ ]  NoIf no, please detail:Click here to enter text. |
|  | **If explicit consent is not being sought, what legal basis enables this data processing?**For more information about conditions for processing, please see the [ICO’s GDPR website](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/). | Personal data (identifiers and potentially identifiable data):[x]  Relating to a contract: Article 6 of GDPR [ ]  Legal obligation: Click here to enter text.[ ]  Vital interests: Click here to enter text.[x]  Public task: Article 6 of GDPR [ ]  Other: Click here to enter text.Special categories of personal data (sensitive data), *if applicable*:[x]  Medical related: Article 9 GDPR [ ]  Public Health: Click here to enter text.[ ]  Employment related: Click here to enter text.[ ]  Vital interests: Click here to enter text.[ ]  Already public: Click here to enter text.[ ]  Legal claim related: Click here to enter text.[ ]  Substantial public interest: Click here to enter text.[ ]  Other: Click here to enter text. |
|  | **Will identifiable data only be handled within the patients’ direct care team (in accordance with the** [**Common Law Duty of Confidentiality**](#CommonLaw)**)?** | [x]  Yes [ ]  NoIf no, please detail:Click here to enter text. |
|  | **How will consent, non-consent, objections or opt-outs be recorded and respected?** | Information will be explained to the service user. Details on how their data is used/processed via the Providers privacy notices. |
|  | **What arrangements are in place to process Subject Access Requests?**What would happen if such a request were made? | All providers are required as part of their other business to be set up for SAR requests, and any such requests regarding this contract would follow the same process. |
|  | **Will the processing of data be automated?**Will the proposed processing of data involved automated means of processing to determine an outcome for the individual? | [ ]  Yes [x]  No[ ]  Not applicableIf yes, please outline what arrangements are available to enable the individual access and to extract data (in a standard file format). Please also detail any profiling that may take place as part through automated processing: Click here to enter text. |
|  | **What process is in place for rectifying/blocking data?**What would happen if such a request were made? | The providers have been required as part of the tender to detail in full their data processes, including storage, security, ability to update/rectify information, remove data and block information. All providers are aware that service users give their consent for their data to be held and used for the purposes of the treatment – this can be retracted at any time, and all providers have confirmed their ability to operate in this way. |
| **Engagement** |
|  | **Has stakeholder engagement taken place?** | [x]  Yes [ ]  NoIf yes, how have any issues identified by stakeholders been considered?CoM were consulted regarding all amendments – concern over inappropriate onward referral to secondary services prompted us to adjust the specification so that such a route must be through the GP. Regarding self-referral and telephone assessment as well as GP advice/information options, the CoM was happy to proceed – it was made clear in the specification that telephone assessment is only for appropriate cases (i.e. where advice/info is needed alone, etc). If no, please outline any plans in the near future to seek stakeholder feedback:Click here to enter text. |
| **Data Sharing** |
|  | **Does the project involve any new data sharing between stakeholder organisations?**  | [ ]  Yes [x]  NoIf yes, please describe:Click here to enter text.Please provide a high level data flow diagram showing how identifiable information would flow. |
| **Data Linkage** |
|  | **Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?**The degree of concern is higher where data is transferred out of its original context (e.g. the sharing and merging of datasets can allow for a collection of a much wider set of information than needed and identifiers might be collected/linked which prevents personal data being kept anonymously) | [x]  Yes [ ]  NoIf yes, please provide a data flow diagram showing how identifiable information would flow and ensure this is added to the CCG Information Asset and Data Flow Register (see Information Assets and Data Flows section).GP MSK provider Repeat referral or referral for  new condition would be linked  by MSK with any previous  knowledge of clientUpdate on client condition and treatment/outcomes from MSK would be added by GP to patient record |
| **Information Security** |
|  | **Who will have access to the data within the project?**Please refer to roles/job titles/organisations. | Patients, MSK providers, GPs (if consent given, when via self-referral). CCG will have access to non-identifiable volume figures.  |
|  | **Is there a useable audit trail in place for the project?** For example, to identify who has accessed a record? | [ ]  Yes [ ]  No[x]  Not applicableIf yes, please outline the audit plan: Click here to enter text. |
|  | **Where will the data be kept/stored/accessed?**Where applicable, please refer to data flow diagram. | GPs will store data on SystmOne/Emiss. MSK providers will store data in their own secure systems (N3 a requirement of the contract). CCG data is not patient identifiable and flow data is therefore stored in the Y drive (Y:\NELCCG\Care Service Delivery & Redesign\Care & Independence\Allied Health Professionals\MSK), outside of a secure folder |
|  | **Please indicate all methods in which data will be transferred** | [x]  Fax [x]  Email (Unsecure/Personal)[x]  Email (Secure/nhs.net) [ ]  Internet (unsecure – e.g. http)[x]  Telephone [x]  Internet (secure – e.g. https)[ ]  By hand [ ]  Courier[x]  Post – track/traceable [x]  Post – normal[ ]  Software [ ]  Mobile app[ ]  Other:  |
|  | **Does the project involve privacy enhancing technologies?***New forms* of encryption, two factor authentication and/or pseudonymisation. | [ ]  Yes [x]  NoIf yes, please give details: Click here to enter text. |
|  | **Is there a documented System Level Security Policy (SLSP) or process for this project?**A [SLSP](#SupportingDocs) is required for new *systems* – this is likely to need to be completed by the supplier. | [ ]  Yes [ ]  No[x]  Not applicableIf yes, please provide a copy. |
| **Privacy and Electronic Communications Regulations** |
|  | **Will the project involve the sending of unsolicited marketing messages electronically such as telephone, fax, email and text?**[Please note that seeking to influence an individual is considered to be marketing.](#PECR) | [ ]  Yes [x]  NoIf yes, what communications will be sent?Click here to enter text.Will consent be sought prior to this?[ ]  Yes [ ]  No n/aIf no, please explain why consent is not being sought first:Click here to enter text. |
| **Records Management** |
|  | **What are the specific retention periods for this data?** Please refer to the [Records Management Code of Practice for Health and 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) and list the retention period for identifiable project datasets. | Adult health records – 8 years Children’s health records - 25th/26th birthday GP records – 10 years after death  |
|  | **Will the data be securely destroyed when it is no longer required?** | [x]  Yes [ ]  NoIf no, please detail: Click here to enter text. |
| **Information Assets and Data Flows** |
|  | **Has an** [**Information Asset Owner**](#IAO) **been identified and does the** [**Information Asset**](#InfoAssets) **and Data Flow Register require updating?**Please see the [Information Asset Register and Data Flow Mapping Form](#SupportingDocs). | [ ]  Yes [x]  NoN/A – the CCG do not hold any identifiable dataIf yes, include the completed Information Asset Register New Entry Form. Does this project constitute a change to existing Information Asset(s) or is this a new Information Asset?[ ]  Yes [x]  NoIf yes, include the completed Information Asset Register and Data Flow Mapping Form for risk review. |
| **Business Continuity** |
|  | **Have the business continuity requirements been considered?** | [x]  Yes [ ]  No[ ]  Business Continuity is not applicablePlease explain and either reference how such plans link with the organisational plan or why there are no business continuity considerations that are applicable for this project: This service is under NHS contract, which requires providers to have a business continuity plan |
| **Open Data** |
|  | **Will identifiable/potentially identifiable from the project be released as Open Data (placed in to the public domain)?** | [ ]  Yes [x]  NoIf yes, please describe: Click here to enter text. |
| **Data Processing Outside of the UK and European Union (EU)** |
|  | **Will any personal and/or sensitive data be transferred to a country outside the UK?** | [ ]  Yes [x]  NoIf yes, which data and to which country?Click here to enter text. |

**Section 3: Data Protection Impact Assessment Information Governance Review**

**Project: MSK**

|  |  |
| --- | --- |
| **Information Governance Review (for completion by IG)** | **Response (for completion by project lead)** |
| **Issue** | **Potential Risk** | **Recommendation** | **Agreed Action** | **Completion (Date and Initials)** |
| **1** | **DPIA –Question 6 -8**No Checks to ensure that the MSK service providers are registered under the Data Protection Act for processing personal identifiable data or whether they have completed an appropriate IG or Data Security and Protection (DSP) Toolkit have been completed. | The CCG being liable for breaches of the Data Protection Act  | All MSK Service Providers to be detailed and the appropriate checks be performed and recorded to show that they have complied with the Data Protection Act and registered with Information Commissioner and completed the appropriate IG Toolkit (Data Security and Protection Toolkit post 31st March) | AchillesDSPT submitted/published ICO No:- Z6404335AscentiDSPT submitted/publishedICO No:- Z2452913Care UKDSPT submitted/publishedICO No:- Z9601307Capital PhysioICO No:- ZA468382Submitted/published (21/11/2019)HS Physiotherapy LtdDSPT –submitted/publishedICO No:- Z3429068In health Group LtdDSPT – Submitted/PublishedICO No:- Z9073906Premier Physical HealthcareDSPT submitted/publishedICO No:- Z1960107Physio-Works DSPT submitted/publishedICO No:- Z346413X AbacusDSPT submitted/publishedICO No:- Z306653XNLAGDSPT submitted/publishedICO No:- Z6405159 |  |
| **2** | **DPIA –Question**  **9**It is not indicated whether the service commissioned has been with a contract that contains the appropriate IG Clauses. | The CCG being liable for breaches of the Data Protection Act due to lack of agreement of processing of personal information allowed | The Model NHS Contract to be used to commission this service and this is to be indicated on the DPIA  | The standard NHS contract has been used.  | Completed |
| **3** | **DPIA –Question**  **13 – 14 & 16**Consent has been recorded as the legal basis to be relied upon for processing this data.Consent is not to be used where an alternative can be applied. | Consent to process an individual’s information can be withdrawn at any point which means the treatment would have to cease | Apply the correct legal basis for processing the information as follows:GDPR Article 6(1)(e) – processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller -The Health Service (Control of Patient Information) Regulations 2002; &GDPR Article 9(2)(h) processing is necessary for the purposes of the provision of health or social care or treatment or the management of health or social care systems and services.However it should be noted that consent will still need to be obtained to meet the common law of confidentiality and demonstrate that the use of personal information has been explained to the service user. | DPIA updated GDPR article 6 & 9To Note - The identified point is not a risk, since the person has chosen to engage with the service and is entitled at any point to discontinue it. They are not under an enforced or recommended course of treatment, and have every right to cease treatment. Information will be explained to the service user. Details on how their data is used/processed via the Providers privacy notices.  | Completed |
| **4** | **DPIA –Question 24 & 26**It is indicated that an audit trail as to how this information has been shared and who has access is not applicable - this is not correct as service users have a right to request who has accessed their information. If as indicated the information is shared via ERS this should facilitate an audit trail | No audit trail would not allow the organisations to fulfil their legal obligations | Ensure that an audit trail is available and record correctly within the DPIAIf referrals and outcomes are transmitted by other means this should be recorded in the patient record. | Comment – AT: The information on service users is not held by the CCG – individual providers hold their own client data. CCG does not get any patient identifiable data – only volume data. While it is absolutely correct that service users have a right to request their information, they would not, therefore, be requesting it from the CCG. Providers can/do use ERS, as well as telephone, email, letter, etc., formats. They will hold assessment data on clients also – this will all be auditable (with the possible exception of the telephone element – however, anything pertinent to the service would be recorded from that on the paperwork). Referrals will always be to GPs, and so would be recorded on the GP’s patient record, if nowhere else. Therefore, this action is complete.  | Completed |
| **5** | **DPIA –Question 32**It must be ensured that the patient data is included on the organisations’ information asset register and a data flow map is completed  | The organisation not meeting its legal requirements under the Data Protection Act  | These information assets may already be recorded and data flow mapped. This needs to be correctly indicated in the DPIA | N/A – the CCG will not hold any identifiable data. Comment – AT: Providers are under the NHS contract, which details appropriate use of data, and the requirement to act according to DPA. The organisations have all signed this contract, and moreover as private companies in their own right are responsible under law for their adherence to DPA | Completed |

*For completion by IG:*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Residual Risk** | **Main Risk Sources** | **Main Threats** | **Main Potential Impacts** | **Main Controls Reducing the Severity and Likelihood** | **Severity** | **Likelihood** |
| **1** |  |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |  |
| **3** |  |  |  |  |  |  |  |

**IG review completed by:**  eMBED Information Governance Specialist **Review date:**  August 2019

**Date complete and risk assessed:** August 2019 **Consultation with ICO required.** No **(delete as appropriate)**

**Section 4: Review and Approval**

**Assessment completed by**

|  |  |
| --- | --- |
| **Name:** | Commissioning Officer  |
| **Title:** | Care and Independence Project Co-ordinator |
| **Date:** | 12/08/2019 |

**Data Protection Officer Approval**

|  |  |
| --- | --- |
| **Name:** | Paul Ellis  |
| **Title:** | NEL CCG Data Protection Officer |
| **DPO advice:**DPO should advise on compliance, risks identified and whether processing can proceed.If accepting any residual high risk, consult the ICO before going ahead | Processing is lawful, fair and transparent with patients fully engaged in the process both in relation to self-referrals or GP referrals. The issues in Section 3 have been addressed, but would make the following points: **Q24** states both Yes / N/A – but issue 4 response identifies that CCG do not have audit trail in place but do not have access to any patient identifiable data; Each provider and GP will have audit trial arrangements in place. **Q26** states that FAX is one of the methods for data transfer, this will need to be phased out in align with NHS requirement to phase out by April 2020. The absence of checks for **Q7** has been addressed by the response to issue 1. Capital Physio have not at the time of the DPIA submitted a DSPT toolkit, though they have agreed to complete by end of August, on this basis Capital Physio should be excluded from the list of providers of MSK Physiotherapy Services until a satisfactory DS&PT toolkit has been completed and published. Further to the points raised I am satisfied that the processing complies with data protection and NHS requirements and that processing as detailed can proceed. |
| **Approved** |[x]
| **Date:** | 30/08/2019 |

The DPO should also review ongoing compliance with DPIA

**SIRO/Caldicott Guardian Approval**

|  |  |
| --- | --- |
| **Name:** | Jan Haxby |
| **Title:** | SIRO |
| **DPO advice accepted or overruled:**If overruled, you must explain your reasons | I agree with DPO comments above. SIRO undertook discussion with IAO in relation to some gaps. These have all been discussed and agreed and DPIA updated accordingly  |
| **Approved:** |[x]
| **Date:** | 10.12.19 |

|  |  |
| --- | --- |
| This DPIA will be kept under review by: |  |