**DPIA Guidance for Completing the OneTrust On-line Form for Social Prescribing Projects**

**Summary**

Each Social Prescribing Pilot Project may require a customised Data Protection Impact Assessment (DPIA) to reflect the specific data processes and local variations involved. This ensures compliance with data protection regulations and supports safe, ethical data sharing.

A ‘Full DPIA’, is required for higher-risk data sharing activities which this document covers. A streamlined version may be used for lower-risk projects. The DPIA is a living document and should be reviewed after 3 years.

A checklist of all the supporting documentation for a DPIA is listed at the end of this document. A DPIA is a live Risk Assessment and can form part of several other Information Governance Documents such as:

- ***Data Processing Agreements (DPAs):*** Define contractual terms for how data is handled between organisations.

***- Information Sharing Agreements (ISAs):*** Outline the purpose and method of data sharing between parties.

***- System Security Policies:*** Technical documentation maintained by NHSG Cyber Security within the Digital Services Team, e.g. for bespoke software supporting the social prescribing pathway.

**Note:** A DPIA is contractual between parties

Process for Completing a DPIA:

1. ***Initial Assessment:*** The Information Governance (IG) Team consults with the project lead to determine if a DPIA is necessary.
2. ***Form Initiation:*** If required, the IG Team launches the OneTrust online DPIA form.
3. ***Form Completion:*** This document provides guidance on how to complete each section, tailored to social prescribing projects.
4. ***Internal Review:*** The completed form should not be submitted immediately. It must first be reviewed by the IG Team and approved by Alan Bell (Head of IG).
5. ***Final Submission:*** Once approved, the DPIA is submitted to Hugh Bishop (Data Controller, NHS Grampian).

Roles and Responsibilities:

* ***NHS Grampian / GP Practice:*** Acts as the *‘Data Controller’* during the referral process.
* ***Third Sector Organisation:*** Becomes the ‘*Data Controller’* once the referral is made.
* ***Service Provider:*** Functions as the *‘Data Processor’*.
* ***GP Link Worker (Connector):*** May be employed externally; any data shared outside NHS Grampian must be clearly identified and documented.

**Note:** In some instances the GP Link Worker (Connector) may not be employed by NHS Grampian and instead by an external provider. The point within the referral process will need to be highlighted when information is shared out with NHS Grampian.

**1.0 - Is a DPIA Legally Required?**

Yes (from initial discussions with IG Team and hence the OneTrust on-line form is generated to the identified project leads)

**1.1. Automated processing, decision-making and/or profiling Is the DPIA legally required? -** *The work involves carrying out a systematic and extensive evaluation of people’s personal details, using automated processing (including profiling). Decisions that have a significant effect on people will be made as a result of the processing.*

**Response:** No, as a clinician is always involved.

**Justification:** None

**1.2 Large scale processing of special category data are we looking at just name and contact details or much more than that?** *- The work involves carrying out large scale processing of any of the special categories of personal data, or of personal data relating to criminal convictions and offences.*

*If simple as Name, Contact Details then not special category data.*

*This section is something to consider when designing the bespoke Social Prescribing Pathway for your project.*

***1. Minimum Data (Always Included): Note: You may have Services signed up to the project who will not take referrals unless they have specific information.***

* *Full name*
* *Contact details (phone, email, address)*
* *Preferred method of contact*

***2. Optional Background Information (With Consent):***

* *Reason for referral (e.g. loneliness, housing issues, mental wellbeing)*
* *Relevant social or health context (e.g. mobility issues, caring responsibilities)*
* *Communication needs (e.g. interpreter required, literacy support)*
* *Any known risks or support preferences*

Considerations - Does the pathway only include name and contact details to be passed on? or is there the possibility background information will be passed to prevent the person/patient sharing their story multiple times? As well as the external organisation being able to accommodate their service to the needs identified in advance?

Another consideration is to confirm whether data gathering and agreeing to share non-identifiable data for the purposes of trend analysis is required e.g. service review/evaluation. Need to answer if it is permissible use of data? This is a very different question than what is trying to be captured by the Risk Assessment within the DPIA.

If for research purposes Caldicott Guardian and potential ethical approvals for the data may be required. For Public Health purposes e.g. audit, monitoring trends or service evaluation need to log it with the Quality Improvement Team. For the purpose of the DPIA it is about the use of personal data not trend analysis.

For pilot projects evaluation would be a key factor and resource, permission for this would need to be obtained.

Is it for 100’s of people? Is large scale over 1,000

Is it a pilot how long for 6mths - probably talking about 100’s of people

Includes:

* Racial or ethnic origin data
* Political opinions data
* Religious or philosophical beliefs data
* Trade Union membership data
* Genetic data
* Biometric data for the purpose of uniquely identifying a person
* Health data
* Sex life or sexual orientation data
* Data which may generally be regarded as increasing risks to people’s rights and freedoms e.g. location data, financial data
* Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive

To decide whether processing is large scale you must consider:

* The number of people affected by the processing, either as a specific number or as a proportion of the relevant population
* The volume of data and/or the range of different data items being processed
* The duration or permanence of the processing
* The geographical extent of the processing activity

**Response:** No

**Justification:** None

**1.3 Monitoring of Publically Accessible Areas** - *The work involves carrying out large scale and systematic monitoring of a publicly accessible area. Includes processing used to observe, monitor or control people*.

**Response:** No

**Justification:** None

**1.4 Matching or combining datasets** – *The work involves matching or combining datasets e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset.*

**Response:** No

**Justification:** None

**1.5 Vulnerable Groups** – *The work involves processing personal data about vulnerable groups. This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data.*

**Response:** Yes

**Justification:** None

**1.6 Significant Innovation or New Technologies** – *The work involves significant innovation or use of a new technology. Examples could include combining use of finger print and face recognition for improved physical access control; new “Internet of Things” applications.*

**Response:** No

**Justification:** None

**1.7 Data transfers** – *The work involves transferring personal data across borders outside of the European Economic Area.*

**Response:** No

**Justification:** None

**1.8 Rights Denial** – *The work involves processing that will prevent people from exercising a right or using a service or a contract. Example: Processing in a public area that people passing by cannot avoid.*

**Response:** No

**Justification:** None

**2.0 3 Step Process**

**2.1 Step One -** **Consultation Phase**

*Consult with all stakeholders about what you wish to do as early as possible in the process. Stakeholders will normally include:*

* *Key service staff e.g. those who will be managing the process.*
* *Technical support, especially if a new system is involved. This may involve the relevant IT supplier.*
* *Information governance advisors e.g. Caldicott Guardian, Information Security Officer, Data Protection Officer.*

*Sometimes it will be necessary to consult with service users. This will be particularly relevant if the change in process will change how they interact with our NHS*

*Board, or what information is collected and shared about them.*

*Early consultation will ensure that appropriate governance and security controls are built into the process as it is being designed and delivered, rather than being ‘bolted on’ shortly before the change is launched.*

**2.2 Step Two- DPIA drafting**

*The responsibility for drafting a DPIA will normally sit with the service area that ‘owns’ the change, however, all stakeholders will have an input. Depending on the nature and complexity of your proposal, more than one service area and/ or Information Asset Owner (IAO) may be the owner(s).*

**2.3 Step Three- Sign-off**

*When a DPIA has been fully completed, it must be submitted for formal review by the Data Protection Officer. To submit a fully completed DPIA you must e-mail the NSS Data Protection mailbox.*

*The Data Protection Officer will review the DPIA to ensure that all information risks are fully recognised and advise whether appropriate controls are in place. They will decide, where the DPIA shows a high degree of residual risk associated with the proposal, whether it is necessary to notify the ICO. It may be necessary to inform and/or involve the Board’s Senior Information Risk Owner (SIRO) as part of this risk assessment and decision-making.*

*For DPIAs which relate to processing/ projects of a risky nature (i.e. it has one or more of the aspects listed in Section One) the Data Protection Officer will aim to*

*respond within 10 working days. For DPIAs which relate to processing/ projects of a less risky nature (i.e. it has none of the aspects listed in the table above) the Data Protection Officer will aim to respond within 15 working days.*

*Once reviewed by the Data Protection Officer, the DPIA will need to be signed off by the Information Asset Owner(s) (IAOs), normally a head of service.*

**3.0 DPIA Questions**

**3.1 – What are you trying to do and why?** *– Give (or attach separately) a high level summary description of the process, including its nature, scope, context, purpose and assets (e.g. hardware, software used, dataflows). Explain the necessity and proportionality of the processing in relation to the purpose(s) you are trying to achieve.*

Add a Business Case ***(Appendix 1)*** or overview of the project into this section.

Need to answer:

* Why is it necessary to do the Social Prescribing?
* Why is it necessary to share the data?
* Is it proportionate as to why you are collecting the data?
* Is the data collected relevant to the Social Prescribing project?

Social Prescribing has a key role in finding an alternative to the standard prescribed medicine. It enables GPs, nurses and other health care professionals to refer people to a range of local, non-clinical services to support their health and wellbeing.

People’s health and wellbeing is determined by a range of social, economic and environmental factors. Social Prescribing places the person at the centre and supports individuals to take greater control of their own health by offering a wide range of social, emotional and practical needs typically available within their local community.

From a local GP Practice level data is required from the Social Prescribing pilot to assess the impact on reduced appointment requests, reduction in pharmacy prescriptions, and reduction on onward secondary care referrals.

From a wider Public Health perspective data would be required to analyse trends across GP patient population groups, to understand gaps in local community service provision and/or limited capacity in geographical areas. This would inform future service design and support policy reform to align resources appropriately to identify needs.

In the event it is agreed for Public Health to gain access to information about the success and impact of the project the following non-identifiable data would include:

* First part of postcode to gather geographical intelligence
* Age
* Gender
* Service Socially Prescribed
* Date Prescribed

If Public Health required additional trend data more so than what the Pilot Project requires then a separate Risk Assessment would be required.

**Note:** The DPIA has to reflect what the process will be. If you can not describe what the Short-Medium and Long-Term data is required it can not be included within the current Risk Assessment ***(Appendix 11).*** Risk Assessment needs to be based on what you know and definite not may want to do’s /aspirational.

Colleagues within Public Health Scotland have confirmed approval would be required to share data out with the Health and Social Care Partnership for pan-Grampian trend analysis. GP Practice would need to agree to share the data.

**Response:**

***<Insert name of GP Practice>*** in partnership with ***<insert name>*** are undertaking a social prescribing project.

Social prescribing is a health pathway that enables GPs and other primary care professionals to refer patients with psychosocial challenges to non-clinical support and activities within their local community.

The service will enable General Practitioners and other healthcare professionals to refer patients to the mental health and wellbeing link worker via SCI Gateway known as a GP Link Worker, the referral pathway which is already used for all referrals to others. The GP Link Worker will contact the patient with the contact details provided in the referral form from the healthcare professionals to carry out the initial assessment with the patient. The next steps will be dependent on this assessment.

The GP Link Worker is employed by NHS Grampian, all necessary confidentiality agreements remain in place for Social Prescribing.

Only relevant data (name, address, date of birth, contact details, reason for referral) within the GP patient record will be shared with the link worker.

The patient will consent to the referral and this will be documented in the patient records in Vision Clinical System.

The software being used will be SCI Gateway referral system and Cegedim Vision.

The GP Link Worker after initial assessment may, with patients agreement, onward refer to the appropriate agency.

The agencies are:

***<insert names of organisations involved with the project>***

If the patient does not agree to the referral they may be sign posted to the above agencies/other agencies for them to self-refer for support.

Only data relevant and necessary to the social prescribing referral will be shared by encrypted email through SCI Gateway to enable the identified individual patient need to be met. Minimum data captured will only be necessary for identification of the patient and referral.

The patient will benefit with an extended holistic approach to their wellbeing and GP practice professionals will be able to offer a wider range of options for their care to the patient, either through referral and/or appropriate signposting, freeing up appointment time for the GP cohort.

Social Prescribing has a key role in finding an alternative to the standard prescribed medicine. It enables GPs, nurses and other healthcare professionals to refer people to a range of local, non-clinical services to support their health and wellbeing.

People’s health and wellbeing is determined by a range of social, economic and environmental factors. Social Prescribing places the person at the centre and supports individuals to take greater control of their own health by offering a wide range of social, emotional and practical needs typically available within their local community.

**3.2 What Personal data will be used? -** Select data subject typesPatients and then manage data elements e.g. name, email etcAdd data subject to add GP practice staff and so on.

**Response:**

**Patients**

***Health Information:*** Additional medical history, GP/Medical Practice details

***Health:*** Registered GP Practice

***Personal Identification:*** CHI, marital status, full name, gender, Date of Birth, sex, age

***Contact Information:*** Personal email, contact details, phone numbers, work email address, mobile phone number, home address

***Background Checks:*** Criminal history

***Criminal Convictions:*** Criminal convictions

***Employment Information:*** Name

***Family Information:*** Personal history

**Agency Staff**

***Contact Information:*** phone numbers, work mobile, contact details, work email address, contact information

***Employment Information:*** name

**GP Practice Staff**

***Contact Information:*** Contact details, contact information, work email address, phone numbers

***Employment Information:*** Name

**NHS Staff**

***Employment Information:*** name

***Contact Information:*** Contact Information, work mobile, work email address, phone numbers, contact details

**3.3. What is the source of the personal data?**

**Response:** Patient NHS Grampian and Cegedim Vision eHealth

**Justification:** None

**3.4 What legal condition for using the Personal data is being relied on? -** *Further guidance can be found at:* [*https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basisfor-processing/*](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basisfor-processing/)

**Response:** 6(1)(e) main one used ‘Processing is the necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.’

**May also include:** 6 (10(a)- ‘Consent of the data subject’ discussed about consent of the data being shared vs consent to be referred to the service provider.

*These are two different aspects and discussed if the patient can still be referred to the service provider even if the patient doesn’t consent for information to be shared.*

*To consider – What is the minimum information e.g. Name and Contact Details for a referral to go ahead?*

*To consider – What method of consent will be used? E.g. patient signs consent for both consent of the referral and consent of data shared.*

**3.5 If using 6(1)(e)** - *If you have identified in the previous question that the legal basis for processing personal data is 6(1)(e), please record here what specific law/regulation this public interest task/authority stems from.*

*For NSS, this will often be a combination of Section 10 of the 1978 NHS Act and a relevant provision from our Functions Order. Any relevant regulation should be quoted.*

**Response:** The basis in law for processing is the Data Protection Act 2018 schedule 1 part 1 para2 and the National Health Service (Scotland) Act 1968 S 2C

**3.6 What legal condition for using Special Category Personal Data is being relied upon?** *Need to pick another legal basis*

**Response:** 9(2)(h) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or contract with a health professional.

**Justification:** Relevant special category personal data held in Vision Clinical System to be shared as part of the referral process.

**3.7 Describe how the personal data will be collected and used -** *Describe how the personal data will be collected, used, transferred and if necessary, kept up to date. This may be attached separately.* See Data Flow Diagram ***(Appendix 12).***

To Consider – Is the process about the patient not having to tell their story multiple times. Referral Form is important and the data you want to capture. Do you want to leave it quite open for the patient to say how much they want to share?

To Consider - Need to agree what model/process is going to be applied with the Social Prescribing Referral Process e.g. could the patient self-refer back to the service provider? Is the service provider reporting back to the GP Practice on patient progress?

There needs to be a detailed explanation how the data is going to be processed.

How does the flow of information work with multiple service providers?

One model for all NHSG delivery may differ tailored to your own pathway.

Understanding your process and looking at each stage. Even though not part of the DPIA there is a requirement to evidence the use of SOPs (Standard OperatingProcedures) to guide colleagues e.g. GP Link Worker administration procedures? Evidence you are doing SOPs’ attach SOPs.

Ideally attach the relevant SOPs ***(Appendix 15 and 16)*** to the DPIA explaining a mitigation action for your DPIA.

**Response:**

Please see attached data flow diagram.

The info to be shared by the SCI Gateway referral to the GP link work, and data to be captured by the GP link worker on referral will be.

Name

Address

Date of birth

CHI Number

Prescription Code

Practice Code

GMC Number

Appropriate/Relevant medical Information only as appropriate to support referral

Patient Contact Details

GP Practice contact details

GP name

Referrals are a one-off process and no further updates will be saved once referral has taken place.

The information captured by the GP link worker will shared with one of the referral agencies detailed in 3.1, will be appropriate and relevant to support that referral

only.

The GP Link Worker role will be able to provide data on the following:

Gender

Age

Registered GP Practice

Assessment outcome

Area of support required

Onward referral destination

Time between receipt of referral & assessment

**3.8 What information is being provided to data subjects? –** *What information is being provided to the people to whom the data relates to ensure that they are aware of this use of their personal data? This is their right to be informed and information such as privacy notices may be included as an attachment.**The regularity body that oversees data protection UK wide is the Information Commissioners Office (ICO). If there are breaches that is reportable to the ICO the NHSG Information Governance Team are involved with this. If a breach happens within a GP practice the GP practice usually reports it to the ICO.*

*Refer to over-arching Organisation Privacy Notice* ***(Appendix 9)*** *e.g. GP Practice will have one for referring patients to secondary care for example. For the new Social Prescribing Pathway/Process probably need to have a bespoke Privacy Notice to include external Service Providers e.g. third sector organisations* ***(Appendix 10).*** *The Service Providers will also be expected to create or have their own privacy notice.*

**Response:** <insert name of GP Practice> Social Prescribing Privacy Notice attached.

Privacy Notice is embedded in GP Practice website <insert web address> and on patient notice board in surgery foyer/waiting area.

**3.9 Individual rights -** *Consider and evidence how an individual's rights in relation to the use of their personal data will be addressed by this process? Rights are not applicable to all**types of processing and expert advice on this may be necessary.*

– IG can provide standard wording

**3.10 Right of access -** *Confirming you have established rights of access for individuals if they want for example a copy of their referral from the GP Practice same with the service provider.*

**Response:** GP Practice standard processes will apply. Individuals can exercise their right of access by making a request to the organisation; this is applicable to any personal data held by the organisation.

**3.11 Right to rectification** – *This is where if you as a patient believe the information is inaccurate e.g. factual information such as inaccurate information about the prescribed medicine. Where it becomes difficult to rectify is when it is clinical opinion or observations at appointments. Need established processes in place for the right to rectification.*

**Response:** GP practice standard processes will apply where applicable to data recorded by the treating health professional.

**3.12 Right to Object (where applicable)**

**Response:** When the GP Practice is processing personal information for the purpose of the performance of a task carried out in the public interest or in the exercise of official authority data subjects have the right to object to the processing and also seek that further processing of their personal information is restricted. Provided the GP Practice can demonstrate compelling legitimate grounds for processing their personal information, for instance; patient safety or for evidence to support legal claims, their right will not be upheld.

**3.13 Right to restrict processing** *– e.g. a clinical letter not happy with contested it restrict access to the document until rectified.*

**Response:** Data Subjects have the right to control how the GP Practice use their personal information in some circumstances. This is known as the right to restriction. When processing is restricted, the GP Practice are permitted to store personal information, but not further use it until an agreement is reached with the data subject about further processing. The GP Practice can retain enough information about the data subject to ensure that their request for restriction is respected in the future. If the GP Practice have shared personal information with any individuals or organisations, if we restrict our processing, we will tell those individuals or organisations about our restriction if it is possible and not an unreasonable amount of effort. Whenever we decide to lift a restriction on processing we will tell the data subject.

**3.14 Right to data portability (where applicable)** – *Not relevant*

**Response:** Not Applicable

**3.15 Right to erasure (where applicable)** *– Not applicable in health, unable to erase information.*

**Response:** Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the ‘right to be forgotten’. The right is not absolute and only applies in certain circumstances. The right to erasure does not apply if processing is necessary for one of the following reasons:

* to exercise the right of freedom of expression and information
* to comply with a legal obligation
* for the performance of a task carried out in the public interest or in the exercise of official authority
* for archiving purposes in the public interest, scientific research historical research or statistical purposes
* where erasure is likely to render impossible or seriously impair the achievement of that processing for the establishment, exercise or defence of legal claims. The GDPR also specifies two circumstances where the right to erasure will not apply to special category data
* if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or · if the processing is necessary for the purposes of preventative or occupational medicine (e.g. where the processing is necessary for the working capacity of an employee
* for medical diagnosis
* for the provision of health or social care or for the management of health or social care systems or services).

**3.16 Right to automated decision-making and profiling (where applicable)** – *Not applicable. Touched on this within one of the earlier screening questions and is not applicable.*

**Response:** Not Applicable

**3.17 For how long will the personal data be kept? -** *Need to look at the Social Prescribing Pathway/Process and also the Scottish Government Records Management that sets out the Retention Schedules for both GP and Health Board. (HSCP will have the Council Retention Schedule)**3yrs after death, 6yrs after NHS Grampian, for GP records for lifetime.**The service provider will have their own retention schedules.*

**Response:** Per the requirements of the SCOTTISH GOVERNMENT RECORDS MANAGEMENT HEALTH AND SOCIAL CARE CODE OF PRACTICE (SCOTLAND) 2020 or Successor document - <https://www.informationgovernance.scot.nhs.uk/wp-content/uploads/2020/06/SG-HSC-Scotland-Records-Management-Code-of-Practice2020>

GP practice holds data in perpetuity.

NHS Grampian holds data in accordance with code of practice. SCI Gateway data is held in perpetuity.

GP Link Worker data is stored on NHS Share Point.

These records are standalone and are not shared unless requested by the patient. Patient access requests can be made through a subject access request in GP surgery for information about the initial referral. Further information on referral can be provided by the link worker using a subject access request through NHS Grampian Clinical Governance.

**3.18 Who will access to the personal data?** - *The GP Practice will have access, the link worker, the service provider and possibly Public Health. Need to be aware of what would be identifiable/non-identifiable data. Data to Public Health for future trend analysis would most likely not be identifiable data. If Name, Address, CHI Number are stripped away it no longer becomes personal data. If only first 4 letters of postcode available it is not necessarily still identifiable data.*

**Response:** GP Practice Staff - access to data required to enable referral to GP link worker.

GP Link Worker - information through SCI Gateway to contact patient for onward referral to third Sector agency.

Then list each partner involved with the Social Prescribing project as follows:

**<insert name of organisation> -** information from GP link worker to enable contact to be made with patient about appropriate activities to meet their needs.

**3.19 Will the personal data be routinely shared with other service any other service or organisation?** *- Relationship between GP and service provider and understanding the difference between Data Controller and Data Processor. The IG Team can help navigate through this.*

*Data Processor - Are you instructing the service provider to deliver this service? this question can cause debate. Are we contracting out part of our service? then it all becomes their data. If an organisation is not happy IG Team can help to navigate whether the service provider becomes the controller or processor.*

*If HSCP is paying for the service does it change? It can do but not the over-riding factor.*

*Is it a Data Controller to a Data Controller or Data Controller to Data Processor? If the organisation is dictating the manor and the purpose they are most likely they are the Data Controller.*

*It is important to get this right to have the right agreement in place to back it up.*

*If it is a Data Controller to a Data Controller sharing of data – It is an Information Sharing Agreement. However, a Data Processing Agreement (DPIA) carries more weight as it refers to liability.*

**Additional Document Required:** [The Information Sharing (IS) Toolkit Approach - Digital Healthcare Scotland](https://www.digihealthcare.scot/our-work/information-governance-and-assurance-branch/information-sharing-toolkit/the-is-toolkit-approach/)

**Response: Yes**

**Justification:** The GP Practice will share personal data with the GP link worker to generate a referral. This will be covered by the Joint Data Controller and Information Sharing Agreement (ISA) ***(see Appendix 14)*** between NHSS Health Board and GPs.

The GP link worker will share data with the Third Sector agency to provide the service to meet the identified referral need of the patient with only

appropriate/relevant data shared to allow this need to be met.

**3.20 Will the personal data be processed by a Data Processor? *–*** *Information Governance can assist and provide examples of a system provider looking after our (NHS Grampian) data but clearly under NHS Grampian instruction.*

**Response:** No

**Justification:** None

**3.21 – 3.29 Organisational Controls -** *Consider and evidence what organisational controls will be in place to support the process and protect the personal data. Need to be assured that the service providers have organisational controls in place to protect the data e.g. training, policies in place, staff confidentiality agreements.*

**NHS Grampian Information Governance Template on ‘Organisation and Technical Controls’ to be completed to include information required for DPIA sections 3.21-3.38**

**3.22 Control – information security and related policy(ices)**

**Response:** NHSG Information Governance & Information Sharing Policies apply and all applicable NHS Scotland (NHSS) policies or its successor e.g. IS, Network Information Systems Regs (NIS), NHSS Records Management Code of Practice (RM CoP).

GP Practice apply all applicable NHS Scotland (NHSS) policies or its successor e.g. Information Sharing, Network Information Systems Regs (NIS), NHSS Records Management Code of Practice (RM CoP), utilising Cegedim Vision for the Clinical system for referral process.

**3.23 Control – staff training**

**Response:** All staff including GP staff complete mandatory Information Governance & Information Sharing training at their Corporate Induction when joining the organisation. They undertake refresher training at every two years and annually respectively.

All staff undertake relevant training required for specific systems e.g. Vision Clinical systems.

**3.24 Control – adverse event reporting and management**

**Response:** NHSG has established internal and external breach reporting mechanisms and processes. Internally this is via Datix (Adverse Event Reporting System). All serious/significant adverse events are also to be reported directly to IG & IS as required as well as reporting through Datix. NHSG reports externally to relevant regulatory bodies (ICO, OSIC, NRS), Professional Medical/Health Bodies (e.g. GMC, NMC, GDC etc.) & Scottish Government (SG) (e.g. NIS) and NCSC as required.

GP Practice uses a toolkit called Enhanced Significant Event Analysis (SEA) to report all serious adverse events. GP Practice reports externally to relevant regulatory bodies (ICO, OSIC, NRS), Professional Medical/Health Bodies (e.g. GMC, NMC, GDC etc.) & Scottish Government (SG) (e.g. NIS) and NCSC as required.

**3.25 Control – physical access and authorisation controls**

**Response:** NHSG only (not applicable to all GPs salaried or independent) – Data Centres accessed via secure swipe cards by authorised NHSG staff only. GP Practice data is securely stored off site by Cegedim Hosted Vision.

**3.26 Control – environmental controls**

**Response:** NHSG Data Centres: Fully tolerant for network and power (back-up connectivity in place and documented in relevant SOPs). Fire suppression systems in place. Temperatures are monitored.

**3.27 Control – information asset management –** *This includes management of backups and asset disposal*

**Response:** Standard NHSG Asset Management policies and protocols apply; these include back-up, information asset logging and disposal. Secure disposal of media is managed via NHSG eHealth with a contract with third party. GP Practice utilise Cegedim for all Asset Management.

**3.28 Control – business continuity**

**Response:** NHSG eHealth Business Continuity Plans are in place. NHSG’s Virtual Server environment is replicated between two data centres including storage. GP Practice Business Continuity plans in place.

**3.29 Control – other** *E.g. Control - Staff contractual. Do all staff hold contracts/confidentiality agreements/are vetted appropriately prior to joining the organisation?*

**Response:** NHSG use standard employee contracts, all staff sign Confidentiality Agreements when joining NHSG and are appropriately vetted (disclosure checks, professional body checks, right to work in UK, references).

GP Practice use standard employee contracts, all staff sign Confidentiality Agreements when joining GP Practice and are appropriately vetted (disclosure checks, professional body checks, right to work in UK, references).

**3.30-3.38 Section on Technical controls –** *consider and evidence what technical controls will be in place to support the process and protect the personal data. This can be captured by a System Security Policy. We are assured that the service providers have technical controls in place to protect the data e.g. password protection.*

*Do It Securely Training?*

*Adverse Event Reporting System – Breach of data incidents*

*Business Continuity Plans and what happens when the system goes down? Back-up procedures.*

*Two-factual Authentication.*

*Review the size of organisations and current controls they may or may not have in place. Some organisations may not be constituted and prefer to remain as an ‘informal sign-posting’ provider.*

*Need to be pragmatic about which organisations would prefer a ‘sign-posted’ approach as opposed to being formal referral provider.*

**3.31 Control – system access levels and user authentication controls**

**Response:**

Standard NHSG controls apply:

* Internet facing to have a minimum standard of 2FA;
* Internal systems to use AD authentication.
* Principle of least privilege applies.

In GP Practice standard Controls apply:

* Cegedim Vision for Clinical
* Internet facing to have a minimum standard of 2FA;
* Internal systems to use AD authentication.
* Principle of least privilege applies.

**3.32 Control – system auditing functionality and procedures**

**Response:** Minimum NHSG standard is all systems/app/processes have robust auditing functionality. Third party access to be audited in addition to standard auditing processes. Minimum GP Practice standard is all systems/app/processes have robust auditing functionality. Third party access to be audited in addition to standard auditing processes.

**3.33 Control – operating system controls -** *This could include vulnerability scanning and anti-virus software*

**Response:** Standard NHSG controls apply for patching and anti-virus scanning in both NHSG and GP Practice Cegidem controls apply for patching the clinical system in the GP Practice.

**3.34 Control – network security** – *This could include firewalls and penetration testing*

**Response:** Standard NHSG controls apply for routine pen testing and network security.

All new systems/apps require pen testing prior to going live; any residual risks will be documented as part of the DPIA and/or SSP.

Standard NHSG controls apply for routine pen testing and network security in GP Practice.

**3.35 Control – encryption of special category personal data**

**Response:**

Standard NHSG controls apply are that all data is to be encrypted to industry accepted standards.

Standard NHSG controls apply are that all data is to be encrypted to industry accepted standards in GP Practice.

**3.36 Control – cyber essentials compliance (if applicable)**

**Response:**

NHSG are not Cyber Essentials compliant.

GP Practice are not Cyber Essentials compliant

**3.37 Control - system security policy (SSP) and standard operating procedures (SOP)**

**Response:**

Not Applicable

**3.38 Control - details of ISO27001/02 accreditation (if applicable)**

**Response:** NHSG are not ISO27001/02 accredited.

**3.39** **Will the personal data be transferred outside the EEA?**

*Will the personal data be transferred outside the European Economic Area (EEA) or countries without an European Commission designated adequate level of protection?*

*If yes, provide details of the safeguards in place for the transfer.*

**Response:** No

**Justification:** None

**3.40 Consultation -** *Describe who has been consulted in relation to this process. For example, subject matter experts, service providers, service users.*

**Response:**

List all representatives e.g. GP Practice Staff, GP Link Worker, Third Sector Organisations, Public Health, NHS Grampian Information Governance

**4.0 Section about Risk**

*Not able to answer this section until you know what the risks are and being able to RAG Status the risk questions.*

**4.1 Data protection principles and risk identification -** *In light of the proposed processing, indicate using the following questions what level of risk has been identified for each of the data protection principles.*

**4.2. Fair, Lawful and Transparent -** *Being informed how we are processing the data. Personal data is processes in a fair, lawful and transparent manner.*

**Response:** Low/Green

**Justification:** None

**4.3 Specific, Explicit and Legitimate Purposes -** *Personal data is collected for specific, explicit and legitimate purposes.**Are we processing the data for specific, explicit and legitimate reasons? – other pieces of legislations may come into play here not just data protection legislation.*

**Response:** Low/Green

**Justification:** None

**4.4. Adequate, Relevant and Limited -** *Personal data is adequate, relevant and limited to what is necessary.**This is about the necessity and proportionate of the data.*

**Response:** Low/Green

**Justification:** None

**4.5 Accurate and kept up to date -** *Personal data is accurate and kept up to date E.g. when referral is done and completed.*

**Response:** Low/Green

**Justification:** None

**4.6 No longer than necessary –** *Personal data is kept no longer than necessary. Review and consider retention schedules*

**Response:** Low/Green

**Justification:** None

**4.7 Adequate Security** *- Personal data is processed in a manner that ensures adequate security. Review Organisational and Technical Controls.*

**Response:** Low/Green

**Justification:** None

**4.8 Risk Assessment upload.**

*A word document that can be completed and attached, mapping out the risks on the table. Applying the 5x5 matrix to score the risk. Include the mitigations for each risk and re-score the risk.*

**Response:** Yes

**Justification:** Please see attached

**Supporting Documentation for a DPIA**

|  |  |  |
| --- | --- | --- |
| **DPIA Ref** | **Item** | **Appendix Ref** |
| 3.1 | Business Case  | Appendix 1 |
| Memorandum of Understanding | Appendix 8 |
| 3.2 | Data Subject Sheet – Personal Data ElementsGP Practice Referral Form to GP Link Worker (via SCI Gateway) | Appendix 4 |
| 3.7 | Process Map | Appendix 3 |
| Data Flow Diagram | Appendix 12 |
| Referral Form from GP Practice to GP Link Worker(via SCI Gateway) | Appendix 4 |
| GP Link Worker Assessment Form  | Appendix 5 |
| GP Link Worker Referral Form to Service Provider | Appendix 6 |
| Standard Operating Procedure for GP Practice | Appendix 15 |
| Standard Operating Procedure for Link Worker | Appendix 16 |
| 3.8 | Social Prescribing Privacy Notice for GP Practice | Appendix 9 |
| Social Prescribing Privacy Notice for Service Providers | Appendix 10 |
| 3.19 | Information Sharing Agreement | Appendix 14 |
| 3.21-3.38 | Organisational and Technical Controls Template | Appendix 17 |
| 4.8 | Risk Assessment Table | Appendix 11 |