Data Protection Impact Assessment (DPIA) Questionnaire for

General Practice Data Collection Project – Phase 1 (Short Term Tool)

August 2019
About the Data Protection Impact Assessment (DPIA)

The DPIA (also known as privacy impact assessment or PIA) is an assessment tool which is used to identify, assess and mitigate any actual or potential risks to privacy created by a proposed or existing process or project that involves the use of personal data. It helps us to identify the most effective way to comply with our data protection obligations and meet individuals’ expectations of privacy. An effective DPIA will allow us to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. Failing to manage privacy risks appropriately can lead to enforcement action from the Information Commissioner’s Office (ICO), which can include substantial fines. The DPIA is just one specific aspect of risk management, and therefore feeds into the overall risk management processes and controls in our organisation.

A DPIA is not a ‘tick-box’ exercise. Consultation may take a number of weeks to complete, so make sure that key stakeholders are engaged early, and that you have enough time prior to delivery to iron out any issues.

Carrying out a DPIA is an iterative process. Once complete, a review date within the next 3 years must be set. Should a specific change in purpose, substantial change in service or change in the law occur before the review date, the DPIA must be re-done?

The ICO code of practice on conducting privacy impact assessments is a useful source of advice.

Is a DPIA required?

Firstly, in order to identify whether you need to carry out a DPIA, you must complete the Screening Questions published on geNSS. A DPIA must be completed for all processes or projects for which the Screening Questions indicate a DPIA is necessary.

Secondly, you must consider the aspects listed in the table below:

- If the process or project that you are planning has one or more of the aspects listed below then it is a LEGAL REQUIREMENT to complete a DPIA at an early stage, as the processing/ project is legally classified of a risky nature. Failure to carry out a DPIA in these circumstances is ILLEGAL.
- If the process or project that you are planning has none of the aspects listed below, but the Screening Questions indicated a DPIA was necessary, you must still continue with a DPIA. Although deemed to be of a less risky nature, completion of a DPIA is a best practice requirement in these circumstances, and provides evidence of our meeting data protection requirements by design and by default.
<table>
<thead>
<tr>
<th></th>
<th>The work involves carrying out a <strong>systematic and extensive evaluation</strong> of people’s personal details, using <strong>automated processing (including profiling)</strong>. Decisions that have a <strong>significant effect</strong> on people will be made as a result of the processing. <strong>Includes:</strong> Profiling and predicting, especially when using aspects about people’s work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements <strong>Processing with effects on people such as exclusion or discrimination</strong> <strong>Excludes:</strong> Processing with little or no effect on people</th>
<th>YES/NO</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>The work involves carrying out <strong>large scale</strong> processing of any of the <strong>special categories</strong> of personal data, or of <strong>personal data relating to criminal convictions and offences</strong>. <strong>Includes:</strong> • 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 <strong>To decide whether processing is large scale you must consider:</strong> • 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</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>The work involves carrying out <strong>large scale</strong> and <strong>systematic monitoring</strong> of a <strong>publicly accessible area</strong>. Includes processing used to observe, monitor or control people.</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>The work involves <strong>matching or combining datasets</strong> 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.</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>The work involves processing personal data about <strong>vulnerable groups</strong>. 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.</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### 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.

### 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).

### 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 nss.dataprotection@nhs.net.

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

<table>
<thead>
<tr>
<th></th>
<th>YES/NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. The work involves <strong>significant innovation</strong> or use of a <strong>new technology</strong>. Examples could include combining use of finger print and face recognition for improved physical access control; new “Internet of Things” applications.</td>
<td>No</td>
</tr>
<tr>
<td>7. The work involves transferring personal data across borders <strong>outside the European Economic Area</strong>.</td>
<td>No</td>
</tr>
<tr>
<td>8. The work involves processing that will <strong>prevent people from exercising a right</strong> or using a service or a contract e.g. processing in a public area that people passing by cannot avoid.</td>
<td>No</td>
</tr>
</tbody>
</table>
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 the table above) the Data Protection Officer will 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 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.

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, assets e.g. hardware, software used, data flows. Explain the necessity and proportionality of the processing in relation to the purpose(s) you are trying to achieve.

NHS National Services Scotland Information Services Division (ISD) has been commissioned by the Primary Care Division of Scottish Government to develop a data collection tool to allow for the collections of data to support (1) the new Scottish General Medical Services Contract negotiations and (2) Primary Care Workforce Planning.

The **2018 Scottish General Medical Services Contract**, a requirement which is set out in The National Health Service (General Medical Services Contracts) (Scotland) Regulations 2018, is a joint agreement between the Scottish Government and the BMA setting out the need for robust and reliable data about general practices. The funding of general practices in Scotland will be reformed and a phased approach is proposed as can be seen in the diagram below:

**Figure 1: Two-phased approach to funding**

<table>
<thead>
<tr>
<th>Phase 1 - contract poll (December 2017)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018/19</td>
</tr>
<tr>
<td>Introduction of a new funding formula</td>
</tr>
<tr>
<td>Increased investment of £23 million</td>
</tr>
<tr>
<td>Start collection of data to inform Phase 2</td>
</tr>
<tr>
<td>2019/20</td>
</tr>
<tr>
<td>GP minimum earnings expectation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase 2 - second contract poll</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020/21</td>
</tr>
<tr>
<td>Guaranteed income range and direct re-imbursement of expenses</td>
</tr>
</tbody>
</table>
To support both new Scottish General Medical Services Contract and workforce planning the Scottish Government and the British Medical Association have agreed that all GP practices will be required to provide the following data to cover a 12 month period:

- **Individual staff data** - job roles, contract type, hours/sessions worked, age and sex.
- **Finance data** - Aggregate information on the income and expense of running a general practice (such as rent, insurance and water), the income of practice staff (including salaried GPs), and the income of GP partners.
- **Workforce data** – Aggregate information on absence (sick leave, maternity / paternity / adoption leave, parental leave and special leave) and vacancy information for in hours staff employed by the GP Practice.

All GP Practices in Scotland will be asked to provide this information. This DPIA relates to Phase 1 only and is for a single, one-off data collection. The intention is to use learning to inform the development of a long term tool to inform further planning phases. A further DPIA will be submitted if this proceeds.

GP Practice data will be inputted and submitted via, a cloud-based platform 'ServiceNow' that is accessed through a Web browser. ServiceNow allows developers to build bespoke applications, such as Forms or Dashboards. This software was recommended by NSS Digital and Security Division.

### 2. What personal data will be used?

<table>
<thead>
<tr>
<th>Categories of individuals</th>
<th>Categories of personal data</th>
<th>Any special categories of personal data [see Guidance Notes for definition]</th>
<th>Sources of personal data</th>
</tr>
</thead>
<tbody>
<tr>
<td>- GPs</td>
<td>Surname and Forename (these</td>
<td>Reason for Leaving the post - options include: 'Death', 'Dismissal', 'Ill-health' (to understand/ investigate potential expenses [which these specific reasons may incur] to the practice and for workforce planning).</td>
<td>GP Practice - Finance and IT Systems</td>
</tr>
<tr>
<td>- Nurses</td>
<td>data items were requested by Users inputting their data in order to assist them in ensuring that the correct staff were recorded and it will only be used to assist the User in keeping track of which staff have/not been inputted rather than</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Other staff involved in direct patient care</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Admin/Non clinical staff</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

1. Source: The 2018 General Medical Services Contract in Scotland
<table>
<thead>
<tr>
<th>Categories of individuals</th>
<th>Categories of personal data</th>
<th>Any special categories of personal data [see Guidance Notes for definition]</th>
<th>Sources of personal data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>just NI number. Although optional, we anticipate that these will be completed for all staff. This information will only be visible to the User inputting their data in their interim saved drafts and will not be included in the final data submission and not collected by NSS).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>National Insurance Number (to support data cleansing prior to analysis/identify individuals who work across more than one practice. Mandatory data item although this information will be removed at the earliest instance once data cleansing is complete and prior to sending the data extract to SG).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sex and age (to understand/investigate sex/age pay disparities and for workforce planning)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Finance - Annual salary, profit share, allowances and expenses information (used to ensure the Minimum Earnings Expectation for GP partners)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Workforce - Contracted hours/sessions,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Categories of individuals</td>
<td>Categories of personal data</td>
<td>Any special categories of personal data [see Guidance Notes for definition]</td>
<td>Sources of personal data</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td>contract type, holiday entitlement (for workforce planning).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The full dataset accompanies this DPIA, and is attached as an excel spreadsheet (Appendix 1).
3. **What legal condition for using the personal data is being relied upon?** [See Guidance Notes for the relevant legal conditions]

<table>
<thead>
<tr>
<th>Legal condition(s) for personal data [see Guidance Notes]</th>
<th>Legal conditions for any special categories of personal data [see Guidance Notes]</th>
</tr>
</thead>
<tbody>
<tr>
<td>6(1)(c) – Processing is necessary for compliance with a legal obligation (The legal gateway is in relation to the NHS (GMS Contracts) (Scotland) Regulations 2018 and the commission of the work by Scottish Ministers to NSS in accordance with Section 10 of the NHS (Scotland) Act 1978)</td>
<td>Article 9 (2) (j) - processing is necessary for statistical purposes in accordance Article 89(1).</td>
</tr>
<tr>
<td>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 (This is in relation to our public tasks which include the provision of evidence for workforce planning)</td>
<td></td>
</tr>
</tbody>
</table>

4. **Describe how the personal data will be collected, used, transferred and if necessary kept up to date – may be attached separately.**

See 'Process/ data flow diagram', on page 12.
Process and data flow diagram

NSS IT
- NHS Board IT Facilitator provided with unique logins for each of their Practices

NHS Boards
- NHS Board IT Facilitator provides unique logins to each of their Practices

GP Practice
- Practice logs onto ServiceNow with their unique login, password is required to be changed on initial login

ServiceNow web-based tool
- Practice saves interim data

ServiceNow temporary table
- Practice saves final data submission

ServiceNow final table
- Forename and Surname removed prior to final data being submitted.

NSS Business Intelligence
- Data extracted

Secure Stats server. PHI analysts
- Data manipulation, such as removing NI number and data cleansing

Secure Stats server. PHI analysts

Stakeholder summary reports – response rate, etc

ISD Workforce Survey publication – aggregate summaries

Scottish Government analysts – unaggregated data extract
Collection of Personal Data

During November 2019 - December 2019 the personal data that will be collected from GP Practices is listed in the 'Individual Staff Members' and 'Leavers' tabs of the data specification spreadsheet attached.

This data will be collected from GP Practices, through manual completion (likely by the Practice Manager) of an electronic web based form in ServiceNow. ServiceNow is currently used by NSS IT as a change and incident management system, and was recommended as the most appropriate tool for the purposes required.

Use of Personal Data

ISD will use these data for:

1. To provide necessary raw data extract to the authorised Scottish Government analysts to carry out analytical work to support contract negotiations (Forename, Surname and NI number data will not be included in this extract);

2. A GP workforce survey publication (based on aggregate data) to inform planning at local and national level;

3. Individual GP Practices will have direct access to the supplied information for their own practice only over the project data collection duration. Access controls will be in place to ensure compliance with information governance.

Transfer of Personal Data

GP Workforce data will be transferred to NSS securely using a web based cloud tool called ServiceNow, which is also, unrelated, used by NHS NSS for many purposes including as an incident monitoring tool and a file management tool. GP practices will be required to log on using a unique password supplied by NSS IT in order to enter and submit data. Details can be found in the access control (section 5.2) of the NSS ServiceNow System Security Policy in Appendix 2.

The ServiceNow data processing addendum can be found in Appendix 3.

Forename and Surname will only be visible to the User inputting their data in their interim saved drafts and will not be included in the final data submission and not collected by NSS.

NI Number will be removed at the earliest instance by NSS once data cleansing by NSS is complete.

The data is sent to a named individual in Scottish Government as an extract via Globalscape. This data extract is not aggregated and will contain all data recorded, aside from Forename, Surname and NI number.

Globalscape is a web based Secure File Transfer Protocol (SFTP) implemented and managed by NHS Scotland National Services Scotland (NSS) to allow the secure transfer of files / data between NSS and trusted / authorised external partners. SG does not have direct access to the ServiceNow system or the data within it.
Kept up to Date

A one-off data submission will be made by every GP Practice to cover a 1-year period, typically from 1st April 2018 to 31st March 2019 (the start and end of the time period may vary slightly for a number of GP practices depending on when they have their own financial start and end year dates).

5. **What information is being provided to the people to whom the data relate to ensure that they are aware of this use of their personal data? – This is the 'right to be informed' and information such as privacy notices may be included as an attachment.**

Commitment to data protection and confidentiality principles are addressed on NHS NSS and Information Services Division websites.

There is a Short Life Working Group which provides governance for the project. Membership includes representatives from BMA and Practice Managers.

See attached contract document (Appendix 4 BMA SG General Practice Contract and Context.). (Referenced in footnote 1, in section 1). All GPs practices have received a letter informing them of the contract, and their duties to provide the data to support this. Section 1 above refers.

A 'Staff Information Leaflet' Appendix 5 has been produced to inform practices staff of the data that will be collected, what personal information will be collected, the use of personal information, the purpose of the data collection, and individuals’ rights.

A 'Principles of Data Confidentiality' document has also been produced by SGPC, which sets out the principles for the confidential handling of these data by SG and NSS. These will be distributed to all GP practices to coincide with the rollout. A copy can be found in Appendix 6.

A 'Data Protection Notice' has been produced (Appendix 7).

6. **How will people’s individual rights in relation to the use of their personal data be addressed by this process? (Rights are not applicable to all types of processing, and expert advice on this may be necessary.)**

Personal information about staff employed by the GP Practice will be collected. The NHS NSS Data Protection Notice recognises the rights an individual has in relation to their personal data and how the organisation operates to ensure these rights are upheld. Additionally, the ISD Data Protection Notice provides more detail on how personal data is used within ISD.
The rights shown below can be exercised (where applicable) by contacting the NSS Data Protection Officer at NSS.DataProtection@nhs.net

**Right of access:**

Although most of what the system holds are Practice-level, aggregate data, the system does hold a small amount of individual level personal data which can be attributed to an individual using the National Insurance number. Should a subject access request be received, it would be possible to arrange for the necessary information from the individual level data to be made available.

Individuals have the right of access to:
- Confirm that their personal information is being held or used by us
- Access their personal information
- See additional information about how we use their personal information

The contact details for individuals wishing to access their personal information is:
NSS Data Protection Officer
Gyle Square
1 South Gyle Crescent
Edinburgh
EH12 9EB
Tel: 0131 275 6000
Email: nss.dataprotection@nhs.net

NI number is a mandatory data item collected to support data cleansing prior to analysis to identify individuals who work across more than one practice. NI number will be removed from the data extract at the earliest instance once data cleansing is complete and replaced with a ‘Primary Key’ (in order to uniquely identify each record in the database in the absence of NI number) prior to analysis or transfer to SG.

**Right to rectification:**

The ServiceNow system has the functionality to delete or replace erroneous data by providing GP Practices the facility to resubmit at any point. It will be the relevant GP Practice responsibility to resubmit the data. NSS will liaise with the relevant data supplier’s data protection officer if a request from a data subject is received directly by NSS.

Individuals have the right to request rectification of personal information we hold about them if it is found to be inaccurate. To do so they should contact the NSS DPO whose contact details are above. Following deletion or replacement of data by a GP Practice in ServiceNow, a new data extract would be extracted to the confidential area on the NSS Stats server and the superseded data extract be deleted.
Right to object (where applicable):

In the event of an objection to capturing information which is submitted to the system, the GP Practice where the data originates from will be the point of contact. GP Practices can discuss this with the individual concerned and, if deemed appropriate, can amend information and resubmit to the system. NSS will liaise with the relevant data supplier’s data protection officer if a request from a data subject is received directly by NSS.

An individual has the right to object to the processing. However whilst a request would be considered it is not an absolute right and is most likely to be overruled on the basis of compelling reasons in relation to the legal gateway provided through the general medical services contract legislation and NSS’s obligations towards Scottish Ministers who have commissioned the collection of the data.

Right to restrict processing (where applicable):

In the event of a desire to restrict processing on the system, the relevant GP Practice data supplier’s data protection officer will be informed so that a proper understanding of the request can be obtained. If the request is deemed appropriate, the GP Practice can amend information and resubmit.

An individual has the right to restrict processing and this would be considered but may be overruled on the basis of compelling reasons in relation to our legal bases for processing. It is not an absolute right and we would review on a case by case basis. NSS has the ability to isolate individual records within the system using appropriate programming codes if it is determined that it is necessary to do so while a decision is being made on how to consider the request.

Right to data portability (where applicable):

Not applicable

Right to erasure (where applicable):

When we process personal information, individuals can exercise their right to erasure. This is not an absolute right and we will review each request on a case by case basis. The request is likely to be overruled as processing is taking place in line with our legal obligations. As above, a data supplier can resubmit if they have wrongly processed an individual’s data.

ServiceNow has the functionality for ISD to delete the information held. Records contained in the data extract on the NSS Stats server can also be searched for and deleted.
**Rights in relation to automated decision-making and profiling** (where applicable):

Not applicable.

**7. For how long will the personal data be kept? - refer to our Document Storage Retention and Disposal Policy for advice**

NI number is a mandatory data item collected to support data cleansing prior to analysis to identify individuals who work across more than one practice. NI number will be removed from the data extract at the earliest instance once data cleansing is complete and replaced with a ‘Primary Key’ (in order to uniquely identify each record in the database in the absence of NI number) prior to analysis or transfer to SG.

Data will be extracted from ServiceNow and stored on the restricted and secure stats server within NHS NSS. Data collected, stored and destroyed will be subject to the [NSS Document Storage, Retention and Disposal Policy](#). ServiceNow has the functionality for ISD to archive and delete the information held.

Agreement between SG and NSS is for personal information for informing the GMS contract negotiations to be destroyed once the negotiating process has concluded (this includes both data held by SG and by NSS) and it is considered that the data is no longer needed. This includes aggregated Individual staff data - job roles, contract type, hours/sessions worked, age and sex - and Finance data - Aggregate information on the income and expense of running a general practice (such as rent, insurance and water), the income of practice staff (including salaried GPs), and the income of GP partners.

NHS NSS PHI often retain indefinitely personal information relating to GP Workforce in accordance with our purposes of public interest in the area of public health (see PTI Record Types, page 48, Section 9, of the NSS Document Storage, Retention and Disposal Policy). In accordance with our retention policy, Workforce data - aggregate information on absence (sick leave, maternity / paternity / adoption leave, parental leave and special leave) and vacancy information for in hours’ staff employed by the GP Practice - and other, aggregated data that will be aggregated by ISD following the data collection will be retained indefinitely for trend analysis purposes.

**8. Who will have access to the personal data?**

**Within NSS:**

Personal data about GP Practice staff will only be accessible to a small number of approved ISD and NSS Digital and Security staff who require access for data processing, data quality control or performing analytics to produce agreed outputs. Access will be subject to permissions being granted by agreed authorisers to the confidential area on the NSS Stats server.
All NHS NSS staff accessing data have completed mandatory information governance training and have signed off the NSS Confidentiality Policy to ensure appropriate understanding of Information Governance principles as well as the Data Protection legislation.

**Outwith NSS:**

The information supplied by GP practices will be held in ServiceNow data centres before being transferred to NSS. Although some ServiceNow employees could have access to personal data, this is governed by the data processing agreement between ServiceNow and NSS in the ServiceNow Data Processing Addendum (Appendix 3).

The NSS ServiceNow System Security Policy (Appendix 2) and the Service Now Data Processing Addendum (Appendix 3) are provided along with this document.

Individual GP Practices will have access to their supplied, draft data for their own practice only over the project data collection duration prior to their final data submission.

A data extract will be provided to Scottish Government in order to perform analysis to support the GP Practice contract negotiations. The data items included in this extract are detailed in the attached spreadsheet (Appendix 1) - all data items are included in this extract apart from Forename and Surname (collected locally in interim saved drafts but not be included in the final data submission and not collected by NSS) and NI Number (removed by NSS once data cleansing is complete prior to sending the data extract to SG). The data extract will be sent via a secure file transfer system used in NSS called Globescape.

The Scottish Government have recently commissioned work on the development of a GP Sustainability Tool. Dependant on timelines, the Sustainability Tool may require access to a limited set of data items collected via the GP Collection Tool. If this is confirmed, an updated DPIA will be provided.

**9. Will the personal data be routinely shared with any other service or organisation? – If yes, provide details of data sharing agreement(s) and any other relevant controls. Advice on data sharing requirements is in the Scottish Information Sharing Toolkit.**

Yes, a raw data extract to the Scottish Government to conduct analyses to support the contract negotiation. As data controllers, Scottish Government have taken appropriate IG advice from their DPO and have agreed a set of ‘Principles of Confidentiality’, these will be made available to every GP Practice and can be found within the Draft Covering letter sent out to all GP practices prior to the start of the data collection. A copy is attached as Appendix 6.
10. **Will the personal data be processed by a Data Processor e.g. an IT services provider?** – [see Guidance Notes for the definition of Data Processor]. If yes, provide details of selection criteria, processing instructions and contract (may be attached separately).

Yes. ServiceNow will be used to capture the data. The NSS ServiceNow Data Processing Addendum (Appendix 3), the NSS ServiceNow System Security Policy (Appendix 2) and NSS Privacy Impact Assessment (Appendix 8) are included along with this document.

11. **Describe what organisational controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary.)**

The following answers apply to NHS NSS staff:

<table>
<thead>
<tr>
<th>Type of Control – examples</th>
<th>Description</th>
</tr>
</thead>
</table>
| Information security and related policy(ies) | Data collection, processing, transfer, storage and retention will be in line with NSS policies.  
All staff on commencement of employment sign an agreement to adhere to information security and its related policy and procedures.  
Will adhere to the NHS Scotland Information Security Policy framework |
| Staff training | Staff analysing or viewing the data will have undergone mandatory IG training – LearnPro IG in Action course and the Medical Research Council Research, GDPR and Confidentiality course.  
Additionally, all staff analysing the data would have undergone statistical disclosure control training. |
| Adverse event reporting and management | If an IG breach were to be detected, staff will report in line with the NSS Adverse Events Management Policy (Appendix 9).  
If NSS become aware of a breach, GP practices will be immediately informed of any potential breaches to their data.  
All NSS staff must follow the Adverse Event Reporting policy, reporting any adverse event such as a security breach within 72 hours of identification. Such events are |
<table>
<thead>
<tr>
<th>Type of Control – examples</th>
<th>Description</th>
</tr>
</thead>
</table>
| Physical access and authorisation controls | Access to raw data on secure NHS NSS servers will be restricted and only approved users will be able to access.  
All staff have unique user identifiers for accessing IT systems, complex passwords, and only NSS devices are allowed access to NSS network and data services. Access to confidential data is reviewed every 6 months with re-authorisation if appropriate.  
All NSS staff are aware of their responsibilities as users of confidential information. |
| Environmental controls | NHS NSS sites have security in place such as CCTV, gated entry into the buildings and encrypted/password protected hardware.  
In rare occasions where personal information is printed, NHS NSS buildings operate a confidential waste policy to ensure breaches do not occur from hard copies.  
NSS have a contractor that is responsible for managing the building where the servers are stored this includes environmental and access controls. |
| Information asset management including management of backups and asset disposal | In line with NSS IT Acceptable Use Policy, permanent erasure of files held on storage devices will only be done by technical IM&T Support staff.  
All data is stored and backed up on secure servers that are off site. The NSS server team manages server backups and storage.  
Existing NSS data retention procedures will be adhered to. NSS has implemented a Document Storage, Retention and Disposal Policy.  
NSS IT Acceptable Use Policy (Appendix 10, Section 11) |
| Business continuity | NSS IT provides support to data recovery for data that has been backed up.  
The NSS Resilience management plan (Appendix 11) covers strategic management response to significant or major business continuity incidents. It |
### Type of Control – examples

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>details actions to ensure NSS can continue to operate at acceptable levels until such time as normal operations are restored.</td>
<td></td>
</tr>
</tbody>
</table>

**Add others where applicable**

---

12. **Describe what technical controls will be in place to support the process and protect the personal data (seek the advice of your Information Security Officer as necessary).**

<table>
<thead>
<tr>
<th>Type of Control – examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System access levels and user authentication controls</td>
<td>Access to raw data on secure NHS NSS servers will be restricted and only approved users will be able to access. Individual log-ins and restricted system and folder access. All users are issued with a unique user identifier with complex passwords. Access to confidential data is reviewed every 6 months and re-authorised where appropriate. All NHS staff are aware of their responsibilities as users of confidential information.</td>
</tr>
<tr>
<td>System auditing functionality and procedures</td>
<td>The NHS IT Acceptable Use Policy states that user activity log ins, internet use, email and system logins are logged and auditable (Appendix 10). The audit data provides the service provider with technical and service usage data in the event of issues or inappropriate user usage/activities. A small number of ISD and NSS IT staff will have access to the GP workforce data to enable them to carry out data profiling, quality checks and to carry out analysis to produce the required outputs. Authorisation to access the data is only available to those granted approval of the data owner, and is only valid for a maximum of 6 months, after which the user is required to apply again to request approval to access to the data. There is a documented audit trail for this process.</td>
</tr>
<tr>
<td>Operating system controls such as vulnerability scanning and anti-virus software</td>
<td>Integrity of information will be maintained and robust measures will be taken to prevent the infection of NHS Scotland computers by malicious software, or malware. The latest versions of approved anti-virus programs will be installed on all systems, desktop and laptop computers and updates implemented immediately they are available.</td>
</tr>
<tr>
<td>Type of Control – examples</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
|                          | - All systems will be updated to the latest identified secure patch or upgrade after these have been assured and tested  
|                          | - Regulatory and legislative requirements will be met |
| Network security such as firewalls and penetration testing | The data is stored on a secure NHS NSS server.  
| | National Services Scotland runs on the N3 network. This offers compressive protection against a wide range of technological threats, including malware. Sophos Antivirus software is used to secure the computer network. This provides a secure web gateway, WIFI, and Email through both antivirus and firewall protection. Sophos antivirus provides both computer and server based protection.  
| Encryption of special category personal data | NSS IT relies on access controls rather than encryption at rest to enhance data security. |
| Cyber Essentials compliance(if applicable) | NSS obtained its Cyber Essentials Certificate on 26 June 2019 (Appendix 12). |
| System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available) | An SSP for ServiceNow is available from NSS IT and is attached with the submission of this DPIA (Appendix 2). |
| Details of ISO27001/02 accreditation (if applicable) | NSS/ ISD are not required to comply with ISO 27001, but with the [NHS Scotland Information Security Policy](http://n3.nhs.uk/technicalinformation/N3NetworkSecurity.cfm) which is in line with ISO 27001. NSS is regularly audited to ensure compliance with the policy |

Add others where applicable

13. Will personal data be transferred to outside the European Economic Area (EEA) or countries without an European Commission-designated adequate level of protection? – If yes, provide details of the safeguards that will be in place for the transfer(s).

No
14. Describe who has been consulted in relation to this process – e.g. subject matter experts, service providers, service users.

There is a Short Life Working Group which has GP and Practice Managers representation on the group (see Appendix 14). The BMA/SGPC represents the majority of GPs and has actively consulting with members. There was a presentation at the Practice Managers’ Conference in May 2019 (see Appendix 15). We have actively linked in and discussed with Senior IG PHI Leads. Pilot work on the data collection tool with a selected number of practices was undertaken in February and again in July.

15. In light of what is proposed, indicate what level of risk has been identified in relation to the following data protection principles:

<table>
<thead>
<tr>
<th>Principle</th>
<th>Low/Green</th>
<th>Medium/Amber</th>
<th>High/Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal data is processed in a fair, lawful and transparent manner</td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal data is collected for specific, explicit and legitimate purposes</td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal data is adequate, relevant and limited to what is necessary</td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal data is accurate, and kept up to date</td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal data is kept no longer than necessary</td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal data is processed in a manner that ensures adequate security</td>
<td>yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 16. Risks and actions identified [see Guidance Notes for more information]. List all that you have identified and ensure that these integrate properly with our NHS Board’s risk management process (‘IRMA’):

<table>
<thead>
<tr>
<th>Description</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Overall Risk rating (L x I)</th>
<th>Mitigation/ Actions</th>
<th>Residual Risk</th>
<th>Risk Owner</th>
<th>Date</th>
</tr>
</thead>
</table>
| Information Governance/ security - There is a risk that information submitted to ISD may be inappropriately viewed, accessed, used or otherwise processed. IG/security breaches may be intentional, accidental or as a result of poor software design, technical error, etc. Breaches can affect patient data, staff data, business data or commercial data. | 2          | 2      | 4                           | • Advice has been obtained from the PHI information governance team.  
  • Data will be securely transferred to ISD using ServiceNow (relevant information governance documentation is available on request)  
  • Outputs will be produced in line with [NSS Statistical Disclosure Control Protocol](https://www.niphq.nhs.uk/documents/documents-56/nss-statistical-disclosure-control-protocol)  
  • Any breaches would be reported in line with IT security policies and appropriate actions taken  
  • The project team have undertaken information governance training  
  • Access to secure stats server will be restricted and access must be applied for and approved by senior members of the project team.  
  • Staff analysing or viewing the data will have undergone mandatory IG training – LearnPro IG in Action course and the Medical Research Council Research, GDPR | 2            | Jonathan Cameron | 07/05/2019       |
Additionally, all staff analysing the data would have undergone statistical disclosure control training.
### 17. Review and Sign-Off

<table>
<thead>
<tr>
<th>Role</th>
<th>Advice/ Action/ Sign-Off</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection Officer (DPO) Advice</td>
<td>Just a few points of clarification needed</td>
<td>27/09/19</td>
</tr>
<tr>
<td></td>
<td>Recommend that before IAO signs off this DPIA that you ensure that the SSP for this project is appropriately completed and up to date.</td>
<td>12/11/2019</td>
</tr>
<tr>
<td>Information Security Officer Advice (questions 11 and 12)</td>
<td>Graeme Stronach</td>
<td></td>
</tr>
<tr>
<td>Others, if necessary e.g. Caldicott Guardian, Senior Information Risk Owner (SIRO)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DPO opinion on whether residual risks need prior notification to the ICO</td>
<td>I don’t believe that the residual risk level will require prior notification</td>
<td>27/09/19</td>
</tr>
<tr>
<td>Information Asset Owner(s) (IAO(s)) Sign Off</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 18. Recommended Review Date:

__________________________________________________________
GUIDANCE NOTES

Question 2 - Special category personal data

The special categories of personal data are specified in Article 9 of the General Data Protection Regulation and include data about:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a person
- health
- sex life or sexual orientation.

Personal data relating to criminal convictions and offences should be regarded as having the same special nature as those in the categories listed above.

Question 3 – Legal condition

It is illegal to process personal data without meeting adequately a legal condition.

For personal data which does not relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list. Please note that ‘data subject’ means the person to whom the personal data relates.

- 6(1)(a) – Consent of the data subject
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 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
- 6(1)(f) – Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

In NHSScotland, in many cases condition 6(1) (e) will be the most relevant.

For personal data which relate to any of the special categories (see definition above) the legal basis for the proposed processing must be one or more from the following list:

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former
members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- 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 a contract with a health professional
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

In NHSScotland, in many cases condition 9(2) (h) will be the most relevant.

The Information Commissioner’s Office (ICO) advises that public authorities will find using consent as a legal basis difficult. So if the proposed processing is to use consent as its legal basis you need to indicate why this is necessary and seek the advice of an appropriate IG professional.

**Question 10 – Data Processor**

Article 4 of the General Data Protection Regulation defines a Data Processor as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller. In practice it includes organisations and companies that provide services such as records storage, transport and destruction and IT services, where we ask them to carry out specific tasks using personal data on our behalf. IT suppliers, even if only accessing data/systems for support issues or bug fixes, are legally defined as a Data Processor. Data Processors may only be used to process personal information where they have provided sufficient guarantees to implement appropriate technical and organisational measures to comply with the law.
Question 16 – Risk Assessment

ASSESSING THE RISK LEVEL

Refer to the NSS Integrated Risk Management Approach (IRMA) – a quick reference guide is published on geNSS - to carry out the risk assessment.

1. Determine the Likelihood (L) of recurrence for the event using the IRMA approach:

The assessment of the current likelihood of a risk occurring should take into account the controls currently in place to prevent it.

When determining the likelihood you should consider:

- The frequency of any previous occurrences e.g. how many times a data breach was reported due to this type of issue (e.g. lost records or records accessed without authorisation) in the last month? In the last year? In the last 5 years?
- You may need to check the Information Governance, Data Protection and Information Security incidents reported in your organisation in order to assess the likelihood.

2. Determine the Impact (I) rating using the IRMA approach:

Look at events that could lead to the impact, not the impact itself

Examples of Events:

- Records lost in transit (e.g. paper records sent by post)
- Information recorded inaccurately or not recorded in the record
- Data not available due to ransom-ware attack
- Data lost due to error in IT systems – no useful backup available.
- Confidential personal data sent by email to wrong addressee
- Confidential personal data made available to external people due to poor role access definition and testing
- New system or changes in a system went life without appropriate change management (new or changes in data processing started without IG approval)

Examples of Impacts:

- Only 1 data subject affected but significant or extreme consequences e.g. missed vital treatment as a consequence of information not being issued to the patient or health professional leading to death or major permanent incapacity.
- Very sensitive data being exposed to people who don’t need to know causes extreme distress (could be patient or staff data).
- Large amount of non-sensitive but personal identifiable data lost in the wind when in transit causing organisational embarrassment in the news for a week.
- Staff snooping neighbours medical records.
- Excessive health data shared with social worker (husband under domestic abuse investigation) causing direct threats and stalking.
- Personal health data shared by a charity with private business for commercial/marketing purposes causing unwanted disturbance.
- Reportable data breach to ICO causing monetary penalty.
- Complaint from patient to ICO results in undertaking for better access to health records.
- 1.6 million Patients in Google Deep mind.
• Compliance Audit recommended.
• DC action required.
• Undertaking served.
• Advisory Visit recommended.
• Improvement Action Plan agreed.
• Enforcement Notice pursued.
• Criminal Investigation pursued.
• Civil Monetary Penalty pursued.

Which impact do you opt for?

NOT worst case scenario

NOT most likely scenario

Opt for the “Reasonably foreseeable, worst case scenario” –

• If you got a phone call to tell you it had happened, you wouldn’t be surprised

3. Determine the \textbf{RISK} rating \( L \times I = R \) using the IRMA approach