



## **Data Protection Impact Assessment (DPIA) Questionnaire for**

COVID 19 Test Data

V1.0

18 August 2020

## DOCUMENT CONTROL SHEET

### Key Information

<b>Title</b>	Covid 19 Test Data
<b>Date Published/ Issued</b>	18 August 2020
<b>Date Effective From</b>	
<b>Version/ Issue Number</b>	V1.0
<b>Document Type</b>	Data Protection Impact Assessment
<b>Document Status</b>	Approved
<b>Author</b>	NHS National Services Scotland (NHS NSS or NSS)
<b>Owner</b>	NHS NSS
<b>Approvers</b>	Security and Architecture Review Board
<b>Contact</b>	
<b>File Name</b>	DPIA Covid 19 Test Data

### Revision History

Version	Date	Summary of Changes
		Note: a data protection rapid assessment was undertaken as an initial review of data protection impact before go-live of the product. This was then developed into this Data Protection Impact Assessment.
		See section 14 for engagement
V0.1	16/06/2020	NHS Scotland IG Leads comments
V0.2	19/06/2020	Updated based on DPO review.
V0.3	27/07/2020	Updated based on DPO review.

### Approvals

Version	Date	Name	Designation
V0.3 (renamed v1.0)	18 August 2020	Security and Architecture Review Board	

## 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.

		YES/NO
1.	The work involves carrying out a <b>systematic and extensive evaluation</b> of people's personal details, using <b>automated processing (including profiling)</b> . Decisions that have a <b>significant effect</b> on people will be made as a result of the processing. <u>Includes:</u> 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 Processing with effects on people such as exclusion or discrimination <u>Excludes:</u> Processing with little or no effect on people	No

		YES/NO
2.	<p>The work involves carrying out <b>large scale</b> processing of any of the <b>special categories</b> of personal data, or of <b>personal data relating to criminal convictions and offences</b>.</p> <p><u>Includes:</u></p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin data</li> <li>• Political opinions data</li> <li>• Religious or philosophical beliefs data</li> <li>• Trade Union membership data</li> <li>• Genetic data</li> <li>• Biometric data for the purpose of uniquely identifying a person</li> <li>• Health data</li> <li>• Sex life or sexual orientation data</li> <li>• Data which may generally be regarded as increasing risks to people's rights and freedoms e.g. location data, financial data</li> <li>• Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive</li> </ul> <p><u>To decide whether processing is <b>large scale</b> you must consider:</u></p> <ul style="list-style-type: none"> <li>• The number of people affected by the processing, either as a specific number or as a proportion of the relevant population</li> <li>• The volume of data and/or the range of different data items being processed</li> <li>• The duration or permanence of the processing</li> <li>• The geographical extent of the processing activity</li> </ul>	Yes
3.	<p>The work involves carrying out <b>large scale</b> and <b>systematic monitoring</b> of a <b>publicly accessible area</b>. Includes processing used to observe, monitor or control people.</p>	No
4.	<p>The work involves <b>matching or combining datasets</b> 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.</p>	No
5.	<p>The work involves processing personal data about <b>vulnerable groups</b>. 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.</p>	Yes
6.	<p>The work involves <b>significant innovation</b> or use of a <b>new technology</b>. Examples could include combining use of finger print and face recognition for improved physical access control; new "Internet of Things" applications.</p>	No
7.	<p>The work involves transferring personal data across borders <b>outside the <a href="#">European Economic Area</a></b>.</p>	No
8.	<p>The work involves processing that will <b>prevent people from exercising a right</b> or using a service or a contract e.g. processing in a public area that people passing by cannot avoid.</p>	No

## **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](mailto: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 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, dataflows). Explain the necessity and proportionality of the processing in relation to the purpose(s) you are trying to achieve.**

This DPIA is the 1st of a set of 4 DPIAs which have been carried out to underpin the change in data processing arrangements made in our organisation, NHS National Services Scotland (NSS) as a result of the Scottish Government's response to the Covid-19 pandemic.

As part of the Scottish Government's response to the Covid-19 pandemic, and to allow NHS Scotland to perform its public health and clinical responsibilities, the results being collected as part of UK Government testing need to be brought into NHS Scotland systems.

The results data then needs to be enriched with patient demographic information to allow the results to be integrated into the right patient records held within a number of NHS Scotland systems. The results data will be enriched with the Community Health Index (CHI) number, full residential address and health board of residence. The required demographic data and the NHS Scotland systems that required the enriched results data will be confirmed through further analysis.

A CHI-AG governance process and PBPP application has been undertaken as part of obtaining the relevant permissions to undertake CHI seeding. There are audit logs of all CHI activity that are recorded and can be used for any investigations or future monitoring. There is an exceptions process for mismatched CHIs.

This proposal is proportionate as it seeks to aggregate all available data on testing at a national level for future use as follows: -

1. understand Covid-19 and the risks to public health, identify trends in Covid-19 and such risks, and control and prevent the spread of Covid-19 and such risks;
2. identify and understand information about patients or potential patients with or at risk of Covid-19, information about incidents of patient exposure to Covid-19 and the management of patients with or at risk of Covid-19 including: locating, contacting, screening, flagging and monitoring such patients and collecting information about and providing services in relation to testing, diagnosis, self-isolation, fitness to work, treatment, medical and social interventions and recovery from Covid-19;
3. understand information about patient access to NHS Scotland services as a direct or indirect result of Covid-19 and the availability and capacity of those services;
4. monitor and manage the response to Covid-19 by NHS Scotland and the Government and the Scottish Ministers including the provision of information to the public about Covid-19 and its effectiveness and information about capacity, medicines, equipment, supplies, services and the workforce within NHS Scotland services;

5. deliver services to patients, clinicians, the NHS Scotland workforce and the public about and in connection with Covid-19, including the provision of information, isolation notes and the provision of NHS Scotland services; and
6. for research and planning in relation to Covid-19.

NSS and PHS will both be a data controller, due to the infrastructure and provision of services by both. They are uniquely placed to coordinate this work. NSS are completing this DPIA as they are facilitating by hosting the data, determining how data will be collected, linked and transferred between relevant systems and processes.

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

<b>Categories of individuals</b>	<b>Categories of personal data</b>	<b>Any special categories of personal data [see Guidance Notes for definition]</b>	<b>Sources of personal data</b>
Patients	Contact details including mobile number and email.  Date of birth and age.  GP details.	Health information - test results	NHS Digital, GPs, Health Boards, Data Subjects.

**3. What legal condition for using the personal data is being relied upon? [see Guidance Notes for the relevant legal conditions]**

<b>Legal condition(s) for <i>personal data</i> [see Guidance Notes]</b>	<b>Legal conditions for any <i>special categories of personal data</i> [see Guidance Notes]</b>
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.	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.  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)

Legal condition(s) for <i>personal data</i> [see Guidance Notes]	Legal conditions for any <i>special categories of personal data</i> [see Guidance Notes]
	<p>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.</p>
<p><b>Article 6(1)e</b> - Schedule 1, Part 1, paragraph 2(1) and 2(2)(d and f) DPA 2018  Section 255(1) and section 256(2) of the Health and Social Care Act 2012 (the 2012 Act). (For more details see Section 255 Request letter)</p> <p><b>For NSS</b> - National Services Scotland (“NSS”) is a Special Health Board operating as per sections 2(f) and 2(j) of the National Health Service (Functions of the Common Services Agency) (Scotland) Order 20082 to provide information, advice and management services in support of the functions of Scottish Ministers, Health Boards and Special Health Boards and to collect and disseminate epidemiological data and participate in epidemiological investigations; and per section 37 and section 10(6) of the National Health Service (Scotland) Act 1978.</p> <p><b>For PHS</b> they are operating as per section 4 of the Public Health Scotland Order 2019 to protect public health including those specified in section 1 of the Public Health etc. (Scotland) Act 2008 (duty of Scottish Ministers to protect public health).</p> <p><b>For NHSScotland Boards</b> they are operating as Health Board under section 1 of the National Health Service (Scotland) Act 1978. The Boards have a statutory responsibility to provide or arrange for the provision of a range of healthcare, health improvement and health protection services.</p> <p><b>Article 9</b> exceptions rely on the following conditions from Part 1 of Schedule 1 of the Data Protection Act 2018:</p> <p>Article 9(2)(h) – Schedule 1, Part 1, paragraph 2(d) and 2 (f) DPA 2018  Article 9(2)(i)- Schedule 1, Part 1, paragraph 3 DPA 2018  Article 9(2)(j) – Schedule 1, Part 1, paragraph 4 DPA 2018</p> <p>The necessity test for these conditions are met due to the processing being necessary:</p> <ol style="list-style-type: none"> <li>1) To have access to the contact details of the data subject in a structured way in order to provide guidance and support</li> <li>2) To provide support necessary to prevent infection and the spread of infection such as health education and information about support services</li> <li>3) To keep individuals and members of the public safe during a public health emergency</li> <li>4) To provide performance aggregate statistics in relation to numbers of contacts made, numbers of unsuccessful contacts, demographic characteristics of contacts, workload management statistics, etc</li> <li>5) To provide data that can inform research into the effectiveness of contact tracing</li> <li>6) To comply with the instructions from Scottish ministers in respect of protecting the</li> </ol>	

<b>Legal condition(s) for <i>personal data</i> [see Guidance Notes]</b>	<b>Legal conditions for any <i>special categories of personal data</i> [see Guidance Notes]</b>
<p>health of the population</p> <p>Section 255(1) and section 256(2) of the Health and Social Care Act 2012 (<b>the 2012 Act</b>). (For more details see Section 255 Request letter)</p> <p><b>For NSS</b> - National Services Scotland (“NSS”) is a Special Health Board operating as per sections 2(f) and 2(j) of the National Health Service (Functions of the Common Services Agency) (Scotland) Order 20082 to provide information, advice and management services in support of the functions of Scottish Ministers, Health Boards and Special Health Boards and to collect and disseminate epidemiological data and participate in epidemiological investigations; and per section 37 and section 10(6) of the National Health Service (Scotland) Act 1978.</p> <p><b>For PHS</b> they are operating as per section 4 of the Public Health Scotland Order 2019 to protect public health including those specified in section 1 of the Public Health etc. (Scotland) Act 2008 (duty of Scottish Ministers to protect public health).</p> <p><b>For NHSScotland Boards</b> they are operating as Health Board under section 1 of the National Health Service (Scotland) Act 1978. The Boards have a statutory responsibility to provide or arrange for the provision of a range of healthcare, health improvement and health protection services.</p>	

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

**The service operates as follows:**

- (a) The existing daily export file containing virology lab results is sent by the ‘ECOSS’ system via the NHS NSS National Integration Hub (NIH), where the CHI matching is done. The UK Data results are sent to NIH.
- (b) Any unmatched CHI will be part of an exceptions process.

The principal technical components are all pre-existing technologies and services used in NHS Scotland, and the practise of using SMS and email for outbound messaging to patients is also established in other services in NHS Scotland. Users of these systems are responsible to ensure that the data contained within each is kept up to date.

Below is a list of all components being used:

**Email** - Email is utilised to obtain login credentials to use the testing referral portals.

**SMS** - Text Functionality to communicate test results via .gov SMS service.

**Website** - The UKG testing programme is booked via the website: <https://www.gov.uk/apply-coronavirus-test> is used for booking tests either as an employer or for self-referral.

**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.**

The following privacy notice provide further information for patients:  
SG privacy notice for Covid 19 Testing can be found here:

<https://www.informationgovernance.scot.nhs.uk/testing-for-covid19-privacy-information/>

SG Covid 19 data general privacy notice can be found here:

<https://www.informationgovernance.scot.nhs.uk/covid-19-privacy-statement/>

The NSS privacy notice can be found here: <https://nhsnss.org/how-nss-works/data-protection/>

The Public Health Scotland privacy notice can be found here:

<https://www.publichealthscotland.scot/our-privacynotice/>

**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.)**

Right of access

Patients normally contact their own health board in the first instance, however, this work will not affect an individual’s right to access their data held by NSS.

Service Now has the capability to comply with this right when requested to do so. Service Now has a process in place that will allow requests to be lodged and processed.

NSS/PHS are responsible to update their own privacy notice where applicable to reflect Covid-19 related work.

Where **NSS** hold any data, then patients can submit a request to access their data via the NSS normal processes. There is more information available in our privacy notice which has been updated and also links to the SG privacy notice.

For NSS: Information is available in the NSS privacy notice which can be accessed at

[https://nhsnss.org/how-nssworks/data-protection/#part5935\\_tab](https://nhsnss.org/how-nssworks/data-protection/#part5935_tab)

For **NHS Boards** including **PHS** You can get more information from their websites.

Right to rectification

The information should be accurate, however, if it's agreed that a patient's personal information is inaccurate or incomplete we'll aim to amend the record(s) within one month, or within two months where the request is complex.

Service Now has the capability to comply with this right when requested to do so. Service Now has a process in place that will allow requests to be lodged and processed.

For NSS: Information is available in the NSS privacy notice which can be accessed at [https://nhsnss.org/how-nssworks/data-protection/#part5935\\_tab](https://nhsnss.org/how-nssworks/data-protection/#part5935_tab)

For **NHS Boards** including **PHS** you can get more information from their websites

#### [Right to object](#) (where applicable)

An individual can object to the processing of their data. However, Controllers do not have to act on their objection where they can demonstrate they have overriding, legitimate grounds for the processing.

Objections are considered on a case by case basis.

Service Now has the capability to comply with this right when requested to do so. Service Now has a process in place that will allow requests to be lodged and processed.

For NSS: Information is available in the NSS privacy notice which can be accessed at [https://nhsnss.org/how-nssworks/data-protection/#part5935\\_tab](https://nhsnss.org/how-nssworks/data-protection/#part5935_tab)

For **NHS Boards** including **PHS** You can get more information from their websites.

#### [Right to restrict processing](#) (where applicable)

An individual has the right to seek restriction of processing of their personal data in a number of circumstances, including where the accuracy of personal data has been contested and where they have objected to the processing of personal data and the Controller is verifying whether they have legitimate grounds that override those of the data subject.

Restrictions are considered on a case by case basis.

Service Now has the capability to comply with this right when requested to do so. Service Now has a process in place that will allow requests to be lodged and processed.

For NSS: Information is available in the NSS privacy notice which can be accessed at [https://nhsnss.org/how-nssworks/data-protection/#part5935\\_tab](https://nhsnss.org/how-nssworks/data-protection/#part5935_tab)

For **NHS Boards** including **PHS** You can get more information from their websites.

#### [Right to data portability](#) (where applicable)

Not applicable.

### Right to erasure (where applicable)

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 reasons of public interest in the area of public health;
- 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; or
- 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 (eg 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 (eg 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). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

Service Now has the capability to comply with this right when requested to do so. Service Now has a process in place that will allow requests to be lodged and processed.

For NSS: Information is available in the NSS privacy notice which can be accessed at [https://nhsnss.org/how-nssworks/data-protection/#part5935\\_tab](https://nhsnss.org/how-nssworks/data-protection/#part5935_tab)  
For **NHS Boards** including **PHS** You can get more information from their websites.

### 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**

The retention period is set at seven years, at which point it will be reviewed. During this time all information will be held in line with:

- Scottish Government Records Management: Health and Social Care Code of Practice 2020; and
- NSS Document Storage, Retention and Disposal Policy v7.3

The current NSS retention schedule version 7.3, is being reviewed in light of the new Scottish Government Records Management: Health and Social Care Code of Practice.

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

**NHS NSS** - NSS will hold the data in the integration hub and are a data controller. The data will be defined as an information asset in the Information Asset Register as the Covid-19 test data. NSS will appropriately share the data with others in order to respond to the pandemic. For each of those sharing purposes, an assessment will be undertaken. This asset will be added to the list of joint assets between NSS and PHS. NSS System support staff will have access should any faults/bugs require action. Practitioner services staff will have access to some data items should they require to manually CHI match. All systems being utilised have role based access controls in place and appropriate auditing functionality for activities undertaken.

**PHS** - This information asset will be held by PHS as a data controller to allow analysis of the data.

**NHS Scotland Boards** as a data controller for data pertaining to their own patients and to view patient test results status.

**NHS Scotland GP's** - PDF reports will be sent to GP's via Ensemble. GP's will only receive a report containing information on patients who are registered with their practice.

#### **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](#).**

NSS will not share the data unless named in this DPIA. Should any future sharing needs be identified. NSS will perform due diligence on whether the sharing is justified, lawful and fair and a full data protection impact assessment will be completed.

#### **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. Server is stored at ATOS data centre in Livingston. It is a secure facility with restricted access and is managed, operated and audited through the NHS Scotland contract. ATOS staff do not have access to the data. There are appropriate contracts and service level agreements in place with ATOS.

#### **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.)**

<b>Type of Control – examples</b>	<b>Description</b>
Information security and related policy(ies)	<p><b>NSS have a suite of policies including but not limited to:</b></p> <ul style="list-style-type: none"> <li>• NSS Access Control Policy V1.2</li> <li>• NSS Clear Desk Policy V1.1</li> <li>• NSS Clear Screen Policy V1.1</li> <li>• NSS Data Classification Policy V.1.0</li> <li>• NSS Email Policy V1.2</li> <li>• NSS Encryption Policy V1.1</li> <li>• NSS Information Security Policy V1.5</li> <li>• NSS Internet Policy V1.1</li> <li>• NSS Mobile Device Policy V1.1</li> <li>• NSS Password Policy V1.1</li> <li>• NSS Remote Access Policy V1.1</li> <li>• NSS Removable Media Policy V1.1</li> </ul> <p><b>Procedures</b></p> <ul style="list-style-type: none"> <li>• Destruction Process for hard drives and mobile phones – CST</li> <li>• NSS Data Cleansing Guidelines</li> <li>• Decommissioning and destruction of IT desktop devices</li> </ul> <p><b>PHS</b> have equivalent policies and procedures in place as well as:</p> <ul style="list-style-type: none"> <li>• Records Management, Document Storage, Retention Policy V1.0</li> <li>• Data Protection Policy V1.0.</li> </ul> <p><b>NHSScotland Health Boards</b> have equivalent policies and procedures.</p> <p><b>Atos</b> is providing the hosting environment including physical space and all corresponding physical and environmental controls, power, SWAN connectivity. Atos are certified to ISO27001 for the provision of IT-services, Consulting Services and business process outsourcing by EY CertifyPoint, ATOS are also contracted to provide services to NHS Scotland.</p>
Staff training	<p>All NSS staff are required to complete mandatory Information Governance training every two years. This is an online module and test. Staff also adhere to the NHS NSS Confidentiality Guidelines V1.1a. Confidentiality also forms part of their employment contract.</p> <p>Staff may be working at home during the pandemic, NSS have issued guidance around this and also have:</p> <ul style="list-style-type: none"> <li>• Working at home and working from home Policy</li> <li>• Remote Access Policy</li> </ul> <p><b>PHS and Health Boards</b> have the equivalent policies and procedures in place, training is given at regular intervals.</p>

Type of Control – examples	Description
	<p><b>All Atos staff</b> complete mandatory security training courses. One of those is a Security Awareness course.</p>
<p>Adverse event reporting and management</p>	<p><b>NSS</b> have an Adverse Events Management Policy and should be followed as appropriate. Staff can report any adverse events via qPulse, our adverse events portal.</p> <p><b>PHS</b> have equivalent policies and procedures in place.</p> <p><b>Health Boards</b> have their own adverse events policies and adverse events systems such as Datix.</p> <p><b>Atos</b> has an account wide incident reporting system that is core to the service delivery management. This system handles all reported incidents and a team of Incident Managers ensures that all incidents are reported back to the necessary Boards and that incidents are resolved in a timely manner.</p>
<p>Physical access and authorisation controls</p>	<p>All <b>NSS</b> staff require an ID pass to scan to enter the building. All systems have secure log on and password requirements. NSS also have:</p> <ul style="list-style-type: none"> <li>• Access Control Policy V1.2 - section 5 page 5.</li> <li>• Clear Desk Policy V1.1 and</li> <li>• NSS Clear Screen Policy V1.1.</li> </ul> <p>All <b>PHS</b> staff require an ID pass to scan to enter the building. All systems have secure log on and password requirements. <b>PHS</b> have equivalent policies and procedures in place.</p> <p><b>NHSScotland</b> Health Boards have equivalent policies and procedures.</p> <p><b>Atos</b> is providing the hosting environment including physical space and all corresponding physical and environmental controls, power, SWAN connectivity. Atos are certified to ISO27001 for the provision of IT-services, Consulting Services and business process outsourcing by EY CertifyPoint, ATOS are also contracted to provide services to NHS Scotland. ATOS do not have access to the data they host.</p>
<p>Environmental controls</p>	<p>Atos is providing the hosting environment including physical space and all corresponding physical and environmental controls, power, SWAN connectivity. Atos are certified to ISO27001 for the provision of IT-services, Consulting Services and business process outsourcing by EY CertifyPoint, ATOS are also contracted to provide services to NHS Scotland.</p>
<p>Information asset management including management of</p>	<p><b>NSS</b> have an information asset register. Information is held in line with the the Scottish Government Records Management Health and Social Care Code of Practice 2020 and NSS Document Storage, Retention and Disposal Policy v7.3.</p>

Type of Control – examples	Description
backups and asset disposal	<p>We also have the following procedures:</p> <ul style="list-style-type: none"> <li>• Destruction Process for hard drives and mobile phones – CST</li> <li>• NSS Data Cleansing Guidelines</li> <li>• Decommissioning and destruction of IT desktop devices</li> </ul> <p><b>PHS</b> have an information asset register and all information is held in line with the the Scottish Government Records Management Health and Social Care Code of Practice 2020. PHS have the same shared policies and procedures in place.</p> <p><b>NHS Scotland Boards</b> have information asset registers and record management plans, as well as holding information in line with the Scottish Government Records Management Health and Social Care Code of Practice 2020.</p> <p><b>Atos</b> All of these areas are within the scope of Atos ISO27001 certifications and are an obligation to them under the contract with NHS NSS.</p>
Business continuity	<p>A disaster recovery plan was produced as part of the project to implement the CDW system and a backup Ensemble server is in place for business continuity. System Security Policies (SSP) exist for CDW and Ensemble.</p> <p>ECOSS SSP is currently being developed, however, the system has been penetration tested and the risks have been actioned.</p> <p>Atos - Standard testing and security risk management is undertaken as part of the contract with ATOS. Disaster Recovery arrangements are covered by the contracted agreement with ATOS which include regular testing of the DR procedure including the confirmation of the efficacy of the DR site.</p>

**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).**

Type of Control – examples	Description
System access levels and user authentication controls	<p>Role based access controls are in place.</p> <p><b>NSS</b> also have the NSS Access Control Policy V1.2:</p> <p><b>PHS</b> and <b>Health Boards</b> have equivalent policies and procedures.</p> <p><b>ATOS</b> are providing the hosting environment including physical space and all corresponding</p>

Type of Control – examples	Description
	<p>physical and environmental controls, power, SWAN connectivity. ATOS will have access to the system to fix any faults or bugs but no access to the data. ATOS have multi-factor authentication and are certified to ISO27001.</p>
<p>System auditing functionality and procedures</p>	<p><b>NSS</b> Information Security Policy V1.5 Section 6 – Responsibilities – page 6-7.</p> <p>All NSS staff work within the NSS Confidentiality Guidelines and should not be accessing information they do not require for work purposes.</p> <p>All NSS staff also follow NSS Incident Reporting procedures and our systems are auditable.</p> <p>There are audit logs of all CHI activity that are recorded and can be used for investigations or future monitoring should there be a data breach or incident.</p> <p><b>PHS</b> and <b>Health Boards</b> have equivalent policies and procedures.</p> <p><b>ATOS</b> has 27001 certifications and as such a wide range of physical and environmental controls apply. These are also governed by the NHS Scotland national contract with Atos</p>
<p>Operating system controls such as vulnerability scanning and anti-virus software</p>	<p><b>NSS</b></p> <p>Information Security Policy V1.5</p> <ul style="list-style-type: none"> <li>• Section 5 – Information Security Policy Principles - page 5-6;</li> <li>• Section 6 – NSS Responsibilities – page 6-7.</li> </ul> <p>End user laptops/computers also have their own virus detection software installed to assist in ensuring local devices are free from viruses.</p> <p><b>PHS</b> have equivalent policies and procedures.</p> <p><b>Health Boards</b> have equivalent policies and procedures.</p> <p><b>ATOS</b> - vulnerabilities are minimised by both regular patching and critical patching. External systems are also scanned for vulnerabilities and mitigations undertaken where necessary. Endpoint Detection and Response systems are also in operation. These are similar to Antivirus solutions but have a broader detection capability than traditional file based signature detection</p>

Type of Control – examples	Description
	<p>systems. Both patching and antimalware compliance is reported on a weekly basis within the delivery review meetings so that any reduction in compliance can be quickly resolved.</p>
<p>Network security such as firewalls and penetration testing</p>	<p>The CDW SSP covers this in detail.</p> <p>The NSS IT Network team will be responsible for the internal network including NSS firewalls. All network traffic, to or from internet based users will be directed through the firewall.</p> <p>The ECOSS SSP is currently being developed, however, penetration testing has been completed and any risks have been actioned.</p> <p><b>ATOS</b> has an extensive range of network security tooling is deployed including traffic segmentation, forward and reverse proxies, multiple firewalls, IPS, IDS, Multi Factor Authentication and other techniques.</p>
<p>Encryption of special category personal data</p>	<p>The data is transferred from NHS Digital to NSS via the Message Exchange for Social Care and Health (MESH). This is the main secure large file transfer service used across health and social care organisations. MESH allows the secure transfer of data via an encrypted link.</p> <p><b>NSS</b> all information assets are encrypted at rest and in transit.</p> <p>NSS Encryption Policy V1.1 covers this in detail.</p> <p><b>PHS</b> have equivalent policies and procedures.</p> <p><b>Health Boards</b> have equivalent policies and procedures.</p>
<p>Cyber Essentials compliance(if applicable)</p>	<p>NSS are working towards Cyber Essentials accreditation.</p>
<p>System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available)</p>	<p>There is an SSP for the Corporate Data Warehouse.</p> <p>There is an SSP for the NSS Ensemble.</p> <p>SSP's for ECOSS and HP Zone are being developed.</p>
<p>Details of ISO27001/02 accreditation (if applicable)</p>	<p>Whilst NSS are not accredited to the specific ISO standard, we work to the NHSS Information Security Management System (ISMS) and general IS policies which are designed by SG to be consistent with this standard.</p> <p>Atos are certified to ISO27001 for the provision of</p>

Type of Control – examples	Description
	IT-services, Consulting Services and business process outsourcing by EY CertifyPoint, ATOS are also contracted to provide services to NHS Scotland.

**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.**

A rapid assessment was completed prior to this full impact assessment.

The Data Protection Officers for NHS National Services Scotland, Public Health Scotland and the Scottish Government have been consulted. National IG leads were also consulted.

The Digital Health and Care Directorate have developed a Data and Intelligence Network to look at the holistic approach to use of data and systems as part of the Covid-19 response and part of that work is looking at how public engagement is developed and undertaken.

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

<i>Principle</i>	<i>Low/ Green</i>	<i>Medium/ Amber</i>	<i>High/ Red</i>
Personal data is processed in a fair, lawful and transparent manner	X		
Personal data is collected for specific, explicit and legitimate purposes	X		
Personal data is adequate, relevant and limited to what is necessary	X		
Personal data is accurate, and kept up to date	X		
Personal data is kept no longer than necessary	X		
Personal data is processed in a manner that ensures adequate security	X		



**16. Risks and actions identified [see Guidance Notes for more information]. List all that you have identified.**

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
1. National project requiring aggregation of significant amounts of data across several technologies, platforms and agencies leading to uncontrolled processing or sharing of personal and special categories of personal data.	3.25	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>• Due diligence in respect of national risk assessments/SSPs completed with appropriate sign-off. ECOSS/HP Zone SSPs being developed.</li> <li>• Due diligence on aggregation and sharing of data completed at national level.</li> <li>• Inter-Board sharing for a clear and defined purpose (response to a public health emergency).</li> <li>• SG Directive letter in force from 22 June establishes standards for inter-Board sharing via implementation of Information Sharing Accord.</li> </ul>	<b>LOW</b>	Public Health Scotland; National Services Scotland; Medical Directors/SIROs, Territorial Boards	19 June 2020
2. Failure of system security leading to data breach.	3.22 3.24 3.25 3.26	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>• Due diligence in respect of national risk assessments/SSPs completed with appropriate sign-off.</li> <li>• Key national system controls</li> </ul>	<b>LOW</b>	Public Health Scotland; National Services Scotland	19 June 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
	3.27 3.28				documented in SSP and DPIA. <ul style="list-style-type: none"> <li>• Territorial Boards deriving assurance from national process/system provider.</li> </ul>			
3. Failure of system leading to data loss.	3.22 3.24 3.25 3.26 3.27 3.28	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>• NSS manage vast quantities of healthcare data national purposes with assurance processes in place.</li> <li>• Existing production systems being used.</li> <li>• National SSPs for systems completed.</li> <li>• Backup processes are in place.</li> </ul>	<b>LOW</b>	Public Health Scotland; National Services Scotland	19 June 2020
4. Lack of understanding amongst public concerning how data processed and why (transparency).	3.8	Likely	Moderate	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>• National privacy notice published.</li> <li>• Additional information published by Territorial Boards.</li> <li>• Widespread public information programme from Scottish Government.</li> </ul>	<b>LOW</b>	Public Health Scotland; National Services Scotland; Medical Directors/SIROs, Territorial Boards	19 June 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
5. Inability of data subjects to exercise their rights in respect of this data.	3.10 3.11 3.12 3.13 3.14 3.15 3.16	Possible	Moderate	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>Assurance will be in place that systems will have the ability to comply with rights where applied.</li> <li>Normal data rights processes apply for all parties.</li> <li>National privacy notice published.</li> <li>Additional information published by Territorial Boards.</li> <li>Widespread public information programme from Scottish Government.</li> <li>Updated privacy notices from Scottish Government.</li> <li>Procedures in place to facilitate for rights compliance</li> </ul>	<b>VERY LOW</b>	Public Health Scotland; National Services Scotland; Medical Directors/SIROs, Territorial Boards	19 June 2020
6. Problems with the accuracy of data used in the process.	3.11	Possible	Moderate	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>Data as recorded by Special and Territorial Boards to be used for main records.</li> <li>Process to correct data available from all parties.</li> </ul>	<b>VERY LOW</b>	Public Health Scotland; National Services Scotland; Medical Directors/SIROs,	19 June 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					<ul style="list-style-type: none"> <li>Exceptions process is in place to assist with both data quality and CHI matching</li> </ul>		Territorial Boards	
8. There is a risk that, due to the lack of physical monitoring of staff activities that naturally takes place in the office space, home-based tracing staff/ their co-residents may make unauthorised copies e.g. take screen shots on their phones etc of patient details, thereby causing a data breach.	3.22 3.23 3.24	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>These risks will be covered by policies and procedures as well as training and guidance for all staff using systems and personal data. This includes a home working and remote access policy. The training has also covered key points around confidentiality when working at home, who may be listening and the breaches this can lead to.</li> <li>Training to be provided to all users.</li> <li>Homeworking policy will be in place.</li> </ul>	<b>LOW</b>	National Services Scotland; Public Health Scotland	3 <sup>rd</sup> July 20
9. Inappropriate access to information due to others living in a	3.22 3.23 3.24	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>Staff will have a username and password that they should not share with others.</li> <li>They will have access to the</li> </ul>	<b>LOW</b>	National Services Scotland	3 <sup>rd</sup> July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
household.					minimum required data in order to complete their tasks. <ul style="list-style-type: none"> <li>• Staff will receive training in regards to data protection and confidentiality. It has been highlighted that it's a disciplinary offence and also a criminal matter as per section 170 of the Data Protection Act 2018.</li> <li>• All user actions are recorded as part of the service of the application audit logs, which can be used for any investigations or incidents.</li> <li>• Homeworking Policy will be in place</li> </ul>			
10. Systems can be at risk from human error at system supplier level (e.g. programming error)	3.11 3.20	Unlikely	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>• Appropriate testing by supplier and users</li> </ul>	<b>LOW</b>	National Services Scotland; Processors	3 <sup>rd</sup> July 20
11. There is a risk that the personal data is used for other	3.1	Unlikely	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>• Data will only be used for the purposes outlined in this DPIA.</li> </ul>	<b>LOW</b>	National Services Scotland; Public	3 <sup>rd</sup> July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
purposes than for what it was originally intended for	3.4 3.5 3.6 3.7 3.20 3.25				<ul style="list-style-type: none"> <li>Any further purposes identified would only be considered if they were compatible with the original purpose.</li> <li>Any further purposes would be subject to a rapid assessment and DPIA.</li> </ul>		Health Scotland	
12. There is a risk that personal data is retained for longer than necessary.	3.17	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>This DPIA exists to ensure that there is due consideration as to the extent of the data used. Service Managers, SIRO's, Information governance staff also have to consider the proportionality and justification for all information that they look to collect initially.</li> <li>Personal data will be kept for 7 years after the last date of recording in line with the <a href="#">Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020</a></li> <li>Pseudonymised data sets will be</li> </ul>	<b>LOW</b>	National Services Scotland; Public Health Scotland; SIRO's	3 <sup>rd</sup> July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					<p>kept for 7yrs after the date that is determined by WHO that Covid-19 is no longer a threat to life. This will facilitate historical research and statistical reporting in the public interest.</p> <ul style="list-style-type: none"> <li>There will be a research value for Covid 19 data, all such requests will be subject to further approvals and independent oversight.</li> </ul>			
13. There is a risk that the personal data is no longer relevant.	3.17	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>Data is subject to the NSS Document Storage, Retention and Disposal Policy v7.3</li> <li>Personal data will be kept for 7 years after the last date of recording in line with the <a href="#">Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020</a>.</li> <li>Data will be Anonymised when possible.</li> </ul>	<b>LOW</b>	National Services Scotland; Public Health Scotland; SIRO's	3 <sup>rd</sup> July 20
14. There is a risk that personal data is passed to external organisations.	3.18 3.19	Unlikely	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>No data will be shared with organisation's other than those listed within this DPIA.</li> </ul>	<b>VERY LOW</b>	National Services Scotland; Public Health Scotland	3 <sup>rd</sup> July 20
15. There is a risk that excessive personal data is collected on an individual.	3.1 3.2	Unlikely	Minor	<b>LOW</b>	<ul style="list-style-type: none"> <li>Datasets have been developed to only collect the information necessary. Datasets provided within the DPIA.</li> </ul>	<b>VERY LOW</b>	National Services Scotland; Public	3 <sup>rd</sup> July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
	3.7						Health Scotland	
16. There could be a Risk of records being incorrectly matched, resulting in the wrong person being contacted and advised of an incorrect test result.	3.7 3.11	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>An exceptions process has been developed to identify any mismatches.</li> <li>The National Integration Hub (Ensemble) performs a Community Health Index (CHI) look up using embedded algorithm within the system which is carried out automatically upon receipt of data.</li> <li>All records i.e. successful and unsuccessful CHI matches are passed to Business Intelligence and ECOSS system, this occurs when the file has finished processing.</li> <li>Any unmatched records, known as 'exceptions', will be flagged for further processing.</li> </ul>	<b>MODERATE</b>	National Services Scotland; Public Health Scotland; SIRO's	3 <sup>rd</sup> July 20
17. Lack of technical or organisational measures implemented to ensure appropriate security of the personal data	3.22 3.24 3.25 3.26 3.27	Possible	Major	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>Well established hosting arrangements testing in controlled environment</li> <li>Procedure for secure transfer of data is documented and followed</li> </ul>	<b>LOW</b>	National Services Scotland; Public Health Scotland; SIRO's; Processors	3 <sup>rd</sup> July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
	3.28 3.31 3.32 3.33 3.34 3.35 3.36 3.37 3.38							
18. Policies may be out of date and therefore lead to misinterpretation of responsibilities where changes may have been made in any updated policy for the time period	3.22	Possible	Moderate	<b>MODERATE</b>	<ul style="list-style-type: none"> <li>Review policies regularly</li> </ul>	<b>LOW</b>	National Services Scotland; Public Health Scotland;	8 <sup>th</sup> July 2020

**17. Review and Sign-Off**

<b>Role</b>	<b>Advice/ Action/ Sign-Off</b>	<b>Date</b>
Data Protection Officer (DPO) Advice	As noted in version control	
Information Security Officer Advice (questions 11 and 12)	Completed prior to approval	
Others, if necessary e.g. Caldicott Guardian, Senior Information Risk Owner (SIRO)	Complete prior to approval	
DPO opinion on whether residual risks need prior notification to the ICO	Not required	
Information Asset Owner(s) (IAO(s)) Sign Off	On approval by SARB	

**18. Recommended Review Date:      Every 6 months**

## **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 live 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 Deepmind.
- 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 **RISK** rating  $L \times I = R$  using the IRMA approach