Data Protection Impact Assessment (DPIA) Questionnaire for

Covid 19 Test Data via BI

V1.0

18 August 2020

DOCUMENT CONTROL SHEET

Key Information

Title	Covid 19 Test Data via BI
Date Published/ Issued	
Date Effective From	
Version/ Issue Number	V1.0
Document Type	Data Protection Impact Assessment
Document Status	Draft
Author	NHS National Services Scotland
Owner	Director, Digital and Security
Approvers	Security and Architecture Review Board
Contact	
File Name	DPIA Covid 19 Test Data via BI

Revision History

Version	Date	Summary of Changes
		Note: a data protection rapid assessment was completed initially for this work and approved. This has been developed into this Data Protection Impact Assessment
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)	29/07/2020	SARB	Security 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 ***systematic and extensive evaluation*** of people's personal details, using ***automated processing (including profiling).*** Decisions that have a ***significant effect*** on people will be made as a result of the processing. Includes: 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 Excludes: Processing with little or no effect on people	No
2.	The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to***	Yes

		YES/NO
	criminal convictions and offences. Includes: • Racial or ethnic origin data • Political opinions data • Religious or philosophical beliefs data • Trade Union membership data • Genetic data • Biometric data for the purpose of uniquely identifying a person • Health data • Sex life or sexual orientation data • Data which may generally be regarded as increasing risks to people's rights and freedoms e.g. location data, financial data • Data processed for purely personal or household matters whose use for any other purposes could be regarded as very intrusive To decide whether processing is ***large scale*** you must consider: • The number of people affected by the processing, either as a specific number or as a proportion of the relevant population • The volume of data and/or the range of different data items being processed • The duration or permanence of the processing • The geographical extent of the processing activity	
3.	The work involves carrying out ***large scale*** and ***systematic monitoring*** of a ***publicly accessible area.*** Includes processing used to observe, monitor or control people.	No
4.	The work involves ***matching or combining datasets*** e.g. joining together data from two or more data processing activities performed for different purposes and/or by different organisations in a way that people would not generally expect; joining together data to create a very large, new dataset.	No
5.	The work involves processing personal data about ***vulnerable groups.*** This includes whenever there is a power imbalance between the people whose data are to be used e.g. children, the mentally ill, the elderly, asylum seekers, and the organisation using their personal data.	Yes
6.	The work involves ***significant innovation*** or use of a ***new technology.*** Examples could include combining use of finger print and face recognition for improved physical access control; new "Internet of Things" applications.	No
7.	The work involves transferring personal data across borders ***outside the European Economic Area.***	No
8.	The work involves processing that will ***prevent people from exercising a right*** or using a service or a contract e.g. processing in a public area that people passing by cannot avoid.	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.

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 4th 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.

   Test data has been received into NHS NSS via Scottish testing labs (and ECOSS) and through NHS Digital for the

   UK testing centres. This data is now required to be used by:

   1. NSS and Public Health Scotland for fulfilment of their functions in relation to public health matters;

   2. By all Health Boards as an immediate need to enable the Health Boards to understand who in their geographic area has been tested for Covid-19. This urgency is compounded by the initiation of the test of the Simple Tracing Tool by NHS Fife, NHS Highland and NHS Lanarkshire. CHIAG granted approval to seed the test data with CHI on 18 May 2020. PBPP approval has also been obtained.

   The purpose of sharing allows the Health Boards to ensure their systems are updated for those who have tested positive and allow further tracing to take place as well as suitable care and support to be made available to those with Covid 19.

   NHS NSS and Public Health Scotland require this information to fulfil their functions as follows:-

   NSS are able to hold, process and use this information by virtue of sections 2(f) and 2(j) of the National Health Service (Functions of the Common Services Agency) (Scotland) Order 2008 to provide information, advice and management services in support of the functions of Scottish Ministers, Health Boards and Special Health Boards; 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.

   PHS 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). Business objects is an application to write reports for each Health Board. Health Boards will be provided with user accounts for business objects in order to run these reports which they will be able to download and use to update systems as well as undertake tracing obligations.

This proposal seeks to enable Health Boards to carry out their functions in relation to the provision of care and support to their patients as well as undertake the new tracing service being piloted by NHS Fife, Lanarkshire and Highland, which will be rolled out to all territorial Health Boards.

This proposal is proportionate as it seeks to aggregate all available data on testing at a national level for use by NHS NSS and Public Health Scotland 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 will be a data controller, due to the infrastructure it provides within NSS and to PHS is uniquely placed to coordinate this work. NSS are facilitating by hosting a lot of the data, determining how data will be collected, linked and transferred between relevant systems and processes.

2. What personal data will be used?

Categories of individuals	**Categories of personal data**	**Any special categories of personal data [see Guidance Notes for definition]**	**Sources of personal data**
Patients	Contact details	Ethnicity, Health data – test results	Data subject, Health Boards, ECOSS, NHS Digital

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

Legal condition(s) for *personal data* [see Guidance Notes]	**Legal conditions for any *special categories of personal data* [see Guidance Notes]**
6(1)(e) - Processing is necessary for the performance of a task carried out in the	9(2)(h) - Processing is necessary for the purposes of preventative or occupational

Legal condition(s) for *personal data* [see Guidance Notes]	**Legal conditions for any *special categories of personal data* [see Guidance Notes]**
public interest or in the exercise of official authority vested in the controller.	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)(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).
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) **Article 6(1)(e)** Schedule 1, Part 1, paragraph 2(1) and 2(2)(d and f) DPA 2018 **Article 9** exceptions rely on the following conditions from Part 1 of Schedule 1 of the Data Protection Act 2018: 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 The necessity test for these conditions are met due to the processing being necessary: 1) To provide support necessary to prevent infection and the spread of infection such as health education and information about support services 2) To provide performance aggregate statistics in relation to numbers of negative/positive cases. 3) To provide data that can inform research into the effectiveness of contact tracing 4) To comply with the instructions from Scottish ministers in respect of protecting the health of the population **For NSS** 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; 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.	

Legal condition(s) for *personal data* [see Guidance Notes]	**Legal conditions for any *special categories of personal data* [see Guidance Notes]**
For PHS 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). **For NHSScotland Boards** 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.	

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

   Test data has been received into NHS NSS via Scottish testing labs (and ECOSS) and through NHS Digital for the UK testing centres.

   In sharing this data, the Health Boards will become data controllers of the data in their own right and will be able to use the data to update their systems accordingly. The Health Boards will receive a daily update to this information. NSS and PHS will use the data in their business objects application to write reports for each Health Board. Health Boards will be provided with user accounts to business objects in order to run these reports which they will be able to download and use to update systems as well as undertake tracing obligations.

   Business Objects report
   The Legacy data has been transferred via spreadsheet through NHS Digital. This transfer was facilitated by SEFT (Secure Electronic File Transfer) or MESH (Message Exchange for Social Care and Health) Digital data is being shared through the secure file transfer service.

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 Scottish Government are engaging with the public which includes television coverage and letters sent to all those considered potential high risk patients. Territorial Boards are also releasing information locally, including additional privacy information where appropriate.

   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/

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

The NSS data protection notice has been updated with a link through to the general SG Covid 19 privacy notice.

The Public Health Scotland privacy notice can be found here: https://www.publichealthscotland.scot/ourprivacynotice/

Individual territorial boards have their own privacy notices available on their websites.

Note it is the responsibility of each board to update their privacy notice, to reflect changes in the use of any data.

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 action a request and 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/hownssworks/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 patients 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 action a request and 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/hownssworks/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. The right to object can also be found (in general terms) in the HBs Privacy Notices. Objections are considered on a case by case basis.

Service Now has the capability to action a request and 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/hownssworks/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. Boards consider such requests on a case by case basis.

Service Now has the capability to action a request and 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/hownssworks/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):

The Right to erasure applies if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation

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 reasons of public interest in the area of public health
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes

- where erasure is likely to render impossible or seriously impair the achievement of that processing; 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 action a request and 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/hownssworks/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

This data will be kept for at least 7 years initially with it being reviewed thereafter. During this time all information will be held in line with:

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

PHS

- Records Management, Document Storage, and Retention Policy V1.0
- Data Protection Policy V1.0

For NHS Boards
Each Board will have their own retention policy which is based on the Records Management: Health and Social Care Code of Practice 2020.

8. Who will have access to the personal data?

NHS National Services Scotland - NSS are the organisation receiving and collating test data and seeding this through CHI. NHS 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, a rapid assessment will be undertaken. NSS will ensure appropriate information governance requirements, including documentation and agreements, are completed as required. This information asset will be held by PHS as a joint controller to allow analysis of the data.

NSS are can collect this information from Department of Health and Social Care (via DHSC Processors) by virtue of sections 2(f) and 2(j) of the National Health Service (Functions of the Common Services Agency) (Scotland) Order 2008 to provide information, advice and management services in support of the functions of Scottish Ministers, Health Boards and Special Health Boards;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.

Public Health Scotland - Organisation as a joint controller with NSS, who are using the data as an anonymised and aggregate data set to model and undertake research on Covid-19 under their functions as well as determining the approach to the pandemic via their public health teams.

NHS Scotland Health Boards - All Scottish Health Boards to run the data against their patient systems to identify those who have had positive tests for track and tracing purposes as well as providing care and support (for example their community care systems).

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 other than as described 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).**

    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.

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.)**

Type of Control – examples	Description

Type of Control – examples	Description
Information security and related policy(ies)	All NHS boards have their own information security and data protection internal policies, that can be requested from IG/DP leads. Policies will be similar to those listed below for NSS. **NSS have a suite of policies including but not limited to:** · NSS Access Control Policy V1.2 · NSS Clear Desk Policy V1.1 · NSS Clear Screen Policy V1.1 · NSS Data Classification Policy V.1.0 · NSS Email Policy V1.2 · NSS Encryption Policy V1.1 · NSS Information Security Policy V1.5 · NSS Internet Policy V1.1 · NSS Mobile Device Policy V1.1 · NSS Password Policy V1.1 · NSS Remote Access Policy V1.1 · NSS Removeable Media Policy V1.1 **Procedures** · Destruction Process for hard drives and mobile phones – CST · NSS Data Cleansing Guidelines · Decommissioning and destruction of IT desktop devices 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.
Staff training	All NHS Scotland staff are required to complete mandatory Information Governance training on a regular basis. This is an online module and assessment via Learn pro or Turas. For NSS staff also adhere to the NHS NSS Confidentiality Guidelines V1.1a. Atos staff complete mandatory security training courses. One of those is a Security Awareness course. Staff are also vetted.
Adverse event reporting and management	NSS have an Adverse Events Management Policy and staff can report any adverse events via qPulse, our adverse events portal. Health Boards have their own adverse

Type of Control – examples	Description
	events policies and adverse events systems such as Datix. **Atos** 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.
Physical access and authorisation controls	All NHS boards have their own information security and data protection internal policies, that can be requested from IG/DP leads, these cover access and authorisation procedures. Policies will be similar to the NSS policies including the Access Control Policy V1.2 - section 5 page 5. All NSS staff require an ID pass to scan to enter the building. All systems have secure log on and password requirements. NSS also have a Clear Desk Policy V1.1 and NSS Clear Screen Policy V1.1. Staff may be working at home during the pandemic, NSS have issued guidance around this and also have: · Working at home and working from home Policy · Remote Access Policy · 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.
Environmental controls	BI is the platform that is used with many data products to enable us to view the data and run and use reports. All infrastructure is hosted by Atos. This location is within scope of the Atos 27001 certification and as such a wide range

Type of Control – examples	Description
	of physical and environmental controls apply. These are also governed by the NHS Scotland national contract with Atos.
Information asset management including management of backups and asset disposal	**NSS** have an information asset register and NSS strive to hold all information in line with the Scottish Government Records Management Health and Social Care Code of Practice 2020 and NSS Document Storage, Retention and Disposal Policy v7.3. We also have the following procedures: · Destruction Process for hard drives and mobile phones – CST · NSS Data Cleansing Guidelines · Decommissioning and destruction of IT desktop devices **PHS** have equivalent polices as listed above and in addition, PHS has: · Records Management, Document Storage, and Retention Policy V1.0 · Data Protection Policy V1.0 **Health Boards** have equivalent or similar policies and procedures. **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.
Business continuity	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.

12. <u>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).</u>

Type of Control – examples	Description
System access levels and user authentication controls	The system has role based access controls. NSS has an Access Control Policy V1.2. **PHS** has an equivalent or similar Access Control Policy. **Health Boards** have equivalent or similar policies and procedures.

Type of Control – examples	Description
	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 do not have access to the data they are hosting.
System auditing functionality and procedures	There are audit logs of the system and CHI activity that can be used for any future monitoring or investigations should a breach or incident be detected. **NSS** - NSS Information Security Policy V1.5 Section 6 – Responsibilities – page 6-7. All NSS staff follow the NSS Adverse Events Management policy. **PHS** - Have equivalent or similar polices. **Health Boards** - Have equivalent or similar polices. **Atos** - Do not have access to the data they are hosting.
Operating system controls such as vulnerability scanning and anti-virus software	All NHS Scotland Health Boards have their own policies and procedures which are similar to the NSS organisational policies covering aspects of system controls listed below: · NSS Information Security Policy V1.5 · Section 5 - Information Security Policy Principles - page 5-6; · Section 6 – NSS Responsibilities – page 6-7. Added to this there is vulnerability scanning and virus detection programmes on desktops as well as any cloud based servers hosting data. Atos - 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 systems. Both patching and antimalware

Type of Control – examples	Description
	compliance is reported on a weekly basis within the delivery review meetings so that any reduction in compliance can be quickly resolved.
Network security such as firewalls and penetration testing	There is SSP's for CDW and Ensemble. 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. Atos - 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. Standard testing and security risk management is undertaken as part of the contract with ATOS.
Encryption of special category personal data	All information assets are encrypted at rest and in transit. NSS also has an Encryption Policy V1.1. **PHS** have equivalent policies in place. **Health Boards** have equivalent policies in place.
Cyber Essentials compliance(if applicable)	NSS are working towards cyber essentials accreditation.
System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available)	There is a SSP for Ensemble and the Corporate Data Warehouse (CDW). There is a SSP for ECOSS being developed, however, penetration testing has been completed and the risks have been actioned.
Details of ISO27001/02 accreditation (if applicable)	NSS are not accredited for this standard, however, we work with reference to the Scottish Government IS policy on ISMS and security etc which is consistent with the standard. 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

Type of Control – examples	Description
	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:**

Principle	***Low/ Green***	***Medium/ Amber***	***High/ Red***
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].

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	**MODERATE**	• Due diligence in respect of national risk assessments/SSPs completed with appropriate sign-off. • Territorial Boards aligning with national programme/requirement. • Due diligence on aggregation and sharing of data completed at national level. • Inter-Board sharing for a clear and defined purpose (response to a public health emergency). • SG Directive in force from 22 June 2020 establishes standards for inter-Board sharing via implementation of Information Sharing Accord.	**LOW**	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	**MODERATE**	• Due diligence in respect of national risk assessments/SSPs completed with appropriate sign-off. • Key national system controls documented in SSP and DPIA.	**LOW**	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				• Territorial Boards deriving assurance from national process/system provider.			
3. Failure of system leading to data loss.	3.22 3.24 3.25 3.26 3.27 3.28	Likely	Moderate	**MODERATE**	• NSS manage vast quantities of healthcare data national purposes with assurance processes in place. • Existing production systems being used. • National SSPs for systems completed. • Backup processes are in place.	**LOW**	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	**MODERATE**	• National privacy notice published. • Additional information published by Territorial Boards. • Widespread public information programme from Scottish Government.	**LOW**	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	**MODERATE**	• Assurance will be in place that systems will have the ability to comply with rights where applied. • Normal data rights processes apply for all parties. • National privacy notice published. • Additional information published by Territorial Boards. • Widespread public information programme from Scottish Government. • Updated privacy notices from Scottish Government. • Procedures in place to facilitate for rights compliance	**VERY LOW**	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	**MODERATE**	• Data as recorded by Special and Territorial Boards to be used for main records. • Process to correct data available from all parties. • Exceptions process is in place to assist with both data quality and	**VERY LOW**	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
					CHI matching		, Territorial Boards	
7. Inadvertent joint controller arrangement established without Article 26 GDPR agreement	3.18	Unlikely	Minor	**LOW**	• SG Directive in force from 22 June 2020 establishes standards and rationale for inter-Board sharing via implementation of Information Sharing Accord.	**VERY LOW**	Scottish Government.	19 June 2020
8. Eavesdropping or disclosure of information due to homeworking. 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	3.22 3.23 3.24	Possible	Major	**MODERATE**	• 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. • Training to be provided to all users. • Homeworking policy will be in place.	**LOW**	National Services Scotland; Public Health Scotland	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
shots on their phones etc of patient details, thereby causing a data breach.								
9. Inappropriate access to information due to others living in a household.	3.22 3.23 3.24	Possible	Major	**MODERATE**	• Staff will have a username and password that they should not share with others. • They will have access to the minimum required data in order to complete their tasks. • Staff will receive training in regards to data protection and confidentiality. • All user actions are recorded as part of the service of the application audit logs. • Homeworking Policy will be in place	**LOW**	National Services Scotland	3rd July 20
10. Systems can be at risk from human error at system supplier level (e.g. programming error)	3.11 3.20	Unlikely	Major	**MODERATE**	• Appropriate testing by supplier and users	**LOW**	National Services Scotland; Processors	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
11. There is a risk that the personal data is used for other purposes than for what it was originally intended for	3.1 3.4 3.5 3.6 3.7 3.20 3.25	Unlikely	Major	**MODERATE**	• Data will only be used for the purposes outlined in this DPIA. • Any further purposes identified would only be considered if they were compatible with the original purpose. • Any further purposes would be subject to a rapid assessment and DPIA.	**LOW**	National Services Scotland; Public Health Scotland	3rd July 20
12. There is a risk that personal data is retained for longer than necessary.	3.17	Possible	Major	**MODERATE**	• 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. • Personal data will be kept for 7 years after the last date of recording in line with the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020 • Pseudonymised data sets will be	**LOW**	National Services Scotland; Public Health Scotland; SIRO's	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					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. • There will be a research value for Covid 19 data, all such requests will be subject to further approvals and independent oversight.			
13. There is a risk that the personal data is no longer relevant.	3.17	Possible	Major	**MODERATE**	• Data is subject to the NSS Document Storage, Retention and Disposal Policy v7.3 • Personal data will be kept for 7 years after the last date of recording in line with the Scottish Government Records Management Health and Social Care Code of Practice (Scotland) 2020. • Data will be Anonymised when possible.	**LOW**	National Services Scotland; Public Health Scotland; SIRO's	3rd July 20
14. There is a risk that personal data is passed to external organisations.	3.18 3.19	Unlikely	Major	**MODERATE**	• No data will be shared with organisation's other than those listed within this DPIA.	**VERY LOW**	National Services Scotland; Public Health Scotland	3rd July 20
15. There is a risk that excessive personal data is collected on an individual.	3.1 3.2	Unlikely	Minor	**LOW**	• Datasets have been developed to only collect the information necessary. Datasets provided within the DPIA.	**VERY LOW**	National Services Scotland; Public	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
	3.7						Health Scotland	
16. 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 3.30 3.31 3.32 3.33 3.34 3.35 3.36 3.37 3.38	Possible	Major	**MODERATE**	• Well established hosting arrangements testing in controlled environment • Procedure for secure transfer of data is documented and followed	**LOW**	National Services Scotland; Public Health Scotland; SIRO's; Processors	3rd July 20
17. Policies may be out of date and therefore lead to	3.21	Possible	Moderate	**MODERATE**	• Review policies regularly	**LOW**	National Services	8th July 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
misinterpretation of responsibilities where changes may have been made in any updated policy for the time period							Scotland; Public Health Scotland;	

17. Review and Sign-Off

Role	Advice/ Action/ Sign-Off	Date
Data Protection Officer (DPO) Advice	See version control information	
Information Security Officer Advice (questions 11 and 12)	Complete 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	

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 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 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 x I = R** using the IRMA approach