Data Protection Impact Assessment (DPIA) Questionnaire for

Simple Tracing Tool (STT)

V1.0

18 August 2020

DOCUMENT CONTROL SHEET

Key Information

Title	Simple Tracing Tool (STT)
Date Published/ Issued	18 August 2020
Date Effective From	
Version/ Issue Number	
Document Type	Data Protection Impact Assessment
Document Status	Approved
Author	NHS National Services Scotland (NHS NSS), Storm ID, DHI
Owner	NHS NSS
Approvers	Security and Architecture Review Board
Contact	
File Name	DPIA Simple Tracing Tool (STT)

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.
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 *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 3rd in 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.

   The scope of this DPIA is 'Simple Tracing Tools', which will be abbreviated in this document as STT Release 0.1.

   The STT technical solution is based on the C19 National Notifications Service ('NNS') which provides a Covid-19 test result service to patients and which has a clinician-facing dashboard / management service. The NNS is driven by the daily lab results data feeds from the Electronic Communication of Surveillance in Scotland ('ECOSS') system which is the established core NHS Scotland service for disseminating laboratory test results, ECOSS is a joint asset of NSS and Public Health Scotland (PHS). The objective of the Covid-19 NNS is to remove a significant burden of NHS effort spent manually notifying patients of Covid-19 test results using lists and outbound calling, allowing instead automatic (or NHS staff triggered) notification to tested patients of their test results. By providing this automation for patients who have offered their contact details, capacity will be freed up within the service, allowing more Covid-19 tests to be taken per day and to allow valuable NHS resources to be directed towards managing patients who test positive.

   The STT extends the NNS architecture to include the ability for NHS Scotland staff conducting contract tracing telephone interviews to enter contact tracing information for those patients with positive results, and to view the submitted contacts and their relative priority level to enable targeted phone-based interviews to be arranged.

   The objective of the STT is to remove a significant burden of manual, paper-based contact tracing from NHS Scotland by providing a degree of automation in the form of electronic capture of contact information volunteered by patients who have tested positive.

   The contact tracers will contact the patients via telephone (mobile or landline), they will perform searches for patients and will ensure they have validated that they have the correct person. Patients are asked about recent contact with others, however, there is no legislative requirement on them to provide this. If they provide the details of others they have been in contact with but do not want their data shared, then all the person who is traced will be told is "that they have been in contact with a positive case and should self-isolate for 14 days". Should false information be provided by individuals as part of this process, there are no powers of recourse in criminal law.

   As confidentiality is paramount in any process where we may utilise personal identifiable information, Staff are expected to be aware of their organisation's confidentiality policy and to comply fully with this while using this service.

   Within STT there is an audit of recent events at the bottom of the page for Index Cases. This can be used for any future investigations should a breach or incident be detected.

CHI is matched on the following variables - Name, Date of Birth, Gender, Postcode. There is an exceptions process for mismatched CHIs. This process ensures the details are searched and matched manually. The manual process has to match on name, date of birth and postcode and all three have to match or it is sent to the contact tracers for them to investigate.

In this release (0.1) of the STT service there is **no patient-facing component**, whether website or dedicated app, and hence no mechanism for tracking devices or to allow patients to enter contact, setting or symptom information. The core NNS service does allow patients to access their test results, for which a dedicated web app 'landing page' is provided to patients (again, no app and no collection of information from patients) but this is not part of the STT.

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 e.g GP appointments.

NSS and PHS will be data controllers. NSS and PHS are uniquely placed to coordinate this work. NSS are completing this DPIA as they are facilitating by hosting a lot of the data, determining how data will be collected, linked and transferred between relevant systems and processes. The service will be deployed in the territorial NHS linked and transferred between relevant systems and processes. The service will be deployed in the territorial NHS Health Boards, who will be Data Controllers, for data relating to patients within their Health Board.

The STT data asset, from which this information will be extracted, is a joint asset held by NSS and PHS. Therefore, as we control the asset, we can determine, in line with our Functions Order, how we are going to use that asset (though we would seek PBPP approval for anything research related). In this case, we are working within section 2(f) 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; 2(j) 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.

This proposal is proportionate as it seeks to use 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.

Reporting and Dashboards

Business Intelligence (BI) is a platform used to view data and run reports. BI will have a full copy of the live DHI database for Management Information (MI) purposes, we will also have the ability to run audit reports from there. There is a separate DPIA for this work named - Covid 19 test data via BI.

There has also been an urgent request to provision dashboards with management information taken from the Simple Tracing tool, such as dashboards showing the number of index cases, the number of contacts traced from those cases and the geographical areas of traced contacts (as examples). These dashboards will be provisioned by information from the STT, which is identifiable, but no person identifiable information will be presented. However, some numbers of positive cases, when linked to geographical area, may be low enough for identification of individuals. NSS use statistical suppression techniques. The management information will be shared with SG, HBs and PHS. HBS and PHS will already have direct access to the information that is feeding the dashboards.

2. <u>**What personal data will be used?**</u>

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	Health data (test results)	Data subject, Health Boards, ECOSS

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

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 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)(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.

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

The Covid-19 Simple Tracing Tool (STT) is a new service being developed as part of the response to the current Covid-19 outbreak.

Article 6(1)e, Schedule 1, Part 1, paragraph 2(1) and 2(2)(d and f) DPA 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.

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.**

The STT service is new (and the underpinning NNS is also new, albeit already approved for live operation), having been devised specifically to provide a digital service specific to the Covid-19 outbreak to complement 'paper and pen' contact tracing services, allowing tracing to be carried out more quickly and at larger scale than would hither to be practicable.

From a contact tracing process perspective, the STT system is an automation aid to the established process of NHS contacting patients whose test results have indicated positive for a given infection. The collection from index cases of their contacts, settings and symptoms, and the recording and use of this information in managing outbreaks is standard practice. The STT system described in this document is specific to Covid-19 tests.

A System Security Policy (SSP) has been completed for this system which contains details of how the service operates.

As confidentiality is paramount in any process where we may utilise personal identifiable information, Staff are expected to be aware of their organisation's confidentiality policy and to comply fully with this while using this service. In this release (0.1) of the STT service there is **no patient-facing component**, whether website or dedicated app, and hence no mechanism for tracking devices or to allow patients to enter contact, setting or symptom information. The core NNS service does allow patients to access their test results, for which a dedicated web app 'landing page' is provided to patients (again, no app and no collection of information from patients) but this is not part of the STT.

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.

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, social media releases 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 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

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 a process in place that will allow requests to be lodged and processed. Storm ID have confirmed that they can comply with any rights requests as the system has the capabilities to do so.

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

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 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

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 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 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

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**

NSS
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. <u>**Who will have access to the personal data?**</u>

NHS National Services Scotland - NSS, as a Data Controller will operate the service on behalf of NHSScotland Boards.

Public Health Scotland are a Data Controller. The service is part of the HPS Covid-19 response measures, ensuring patients who have a test result for the virus are informed through digital channels, and patients who test positive can be informed and given advice and treatment promptly by NHSS staff. All systems being utilised have role based access controls in place and appropriate auditing functionality for activities undertaken.

Health Boards - Data controllers of data relating to patients accessing NHS care within their territorial NHS board geographical areas. Territorial Health Boards whose testing teams use the service, do so to:
- Input patient contact information (telephone number and email address)
- View patient test results status (positive, negative, and whether a patient has accessed their result).

Patients who have not accessed their information within a set maximum time will be contacted to advise them of their test result. All systems being utilised have role based access controls in place and appropriate auditing functionality for activities undertaken.

Users are provided with a login account to the platform which is accessed via the clinical dashboard application. For each Health Board, a 'superuser' will be nominated by the Board. The superuser account will be created by Storm. The superuser account is created with a fixed set of privileges, which is the set of information search, view, update privileges that are accorded to all clinical users, with the addition of the capability to add or remove clinical users for their own Health Board domain only.

Additional clinical users will be provisioned (and removed from the system when required) by the superuser. For all non-superuser accounts, the privileges are granted the same: there is only one 'profile', with the exception that clinical users are able to access only the patient information from their own Health Board.

The data platform providing patient information storage and processing is an Internet-based digital platform currently hosted on NHSGGC Azure infrastructure and used to provide digital services supporting existing processes. All systems being utilised have role based access controls in place and appropriate auditing is completed every six months. The auditing system will be reviewed for access and notifying of, and/or acting upon suspicious or unusual activity.

9. <u>**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.](#)**</u>

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).**

NHS National Education for Scotland - Manages the National Digital Platform (NDP).

StormID Ltd – Manages the data platform providing patient information storage and processing.

Sitekit Ltd – second line support (problem ticket management and testing). No routine access to PII.

Gov.uk Notify (UK Government Digital Service) – subcontractor to Storm ID Ltd. Within the NNS, the Notify service provides outbound SMS and email messages to patients advising them to log in to the NNS to view their Covid-19 results.

Microsoft Azure NHS Scotland Azure Environment. Microsoft Azure has completed Level 2 of the NHS IG Toolkit. (https://download.microsoft.com/download/7/F/6/7F6EBDDE-F3EF-4225-ACDAADCD851430C4/NHS_IGCompliance.pdf)"

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
Information security and related policy(ies)	**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 Simple Tracing Tool SSP **Procedures** • Destruction Process for hard drives and mobile phones – CST • NSS Data Cleansing Guidelines • Decommissioning and destruction of IT desktop devices **PHS** has equivalent polices as listed above, in

Type of Control – examples	Description
	addition PHS has: • Records Management, Document Storage, and • Retention Policy V1.0 Data Protection Policy V1.0 • **Health Boards -** Each Health Board will have equivalent polices as listed above. **Microsoft Azure** - NHS Scotland Azure Environment. Microsoft Azure has completed Level 2 of the NHS IG Toolkit. **Storm ID -** Storm ID is Cyber Essentials Plus certified. The solution adheres to the five technical controls of Cyber Essentials: · Secure your Internet connection · Secure your devices and software · Control access to your data and services · Protect from viruses and other malware · Keep your devices and software up to date The solution is deployed to the Azure public cloud where it does not have any access to network traffic on shared networks. Solution components that integrate with other systems are protected with both application level and network level security to prevent unauthorised network access to the destination infrastructure. This uses a combination of controls including WAF, NSG and keystore protected authentication.
Staff training	**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. **PHS** staff are required to complete mandatory Information Governance Training and have equivalent policies and procedures. **NHS Scotland** staff also receive mandatory IG training and Confidentiality also forms part of their employment contract. **Microsoft Azure** staff are trained to ensure they meet their own legal obligations and the contractual requirements. **Storm ID** - staff are vetted and trained to ensure they meet their own legal obligations and as per the contractual requirements.
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. **PHS** have equivalent policies and procedures. **Health Boards** have their own adverse events

Type of Control – examples	Description
	policies and adverse events systems such as Datix. **Processors** - Our contracts and agreements include data protection provisions for data and security breaches.
Physical access and authorisation controls	**NSS** have identify management systems, including role based access, in place. Further details can be found in the NSS Access Control Policy V1.2. During this pandemic staff will be working from home. NSS has a policy which covers home and remote working. There has been guidance issued to help staff understand the risks of working from home. Staff can also use secure VPN connection (if they have one). NSS have the following policies: • Working at home and working from home Policy • Remote Access Policy 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. **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. **Microsoft Azure** have equivalent or similar policies to ensure they meet their own legal obligations and the contractual requirements. **Storm ID** staff are vetted and trained. Storm ID have equivalent or similar policies to ensure they meet their own legal obligations and the contractual requirements.
Environmental controls	**NDP** - The NDP is hosted in the Microsoft Azure Cloud. Online resources describing the physical security and compliance can be found at: https://www.microsoft.com/en-gb/cloud-platform/global-datacenters . The Routing Service sits in the NDP and so is also hosted in the Microsoft Azure Cloud. **ECOSS** - SSP being developed, however, penetration testing has been completed and the risks highlighted have been actioned.

Type of Control – examples	Description
	NIH/Ensemble - All infrastructure is hosted by Atos. This location is within scope of the Atos 27001 certification and as such a wide range of physical and environmental controls apply. These are also governed by the NHS Scotland national contract with Atos. **StormID Ltd** – The data platform providing patient information storage and processing an Internet-based digital platform currently hosted on NHSGGC Azure infrastructure and used to provide digital services. **Microsoft Azure** has completed Level 2 of the NHS IG Toolkit.
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. **Storm ID** IT team are responsible for maintaining Information Backup controls. All business-critical data is backed-up and restores are tested on a schedule. All data held within backup and DR environments is provided the same security and protection as data held in live data stores. Where possible, cloud resources of any kind are geographically housed and/or replicated, across multiple regions, to provide a highly available solution. In the case of data stores – Storage or Database (both of which will be designed in a Highly Available fashion) – regular snapshots of data, built-in 'Point-in-time-Recovery' up to 35 days, and fully customisable long-term retention policies of both, offer a unique software-defined backup and DR solution for any application. **Azure** Devops CI/CD pipelines, including templated Infrastructure as Code (IaC) ensures that, in the case of Disaster Recovery, both

Type of Control – examples	Description
	infrastructure and application code can be redeployed to a previously known and working state in minutes. DR scenarios and RPOs/RTOs are factored into solutions where necessary
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. A SSP for ECOSS is being developed, however, penetration testing has been completed and the risks highlighted have been actioned. There is an SSP for Simple Tracing Tool (STT) and a SSP for the NDP routing service.

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	**NSS** - The system has role based access controls. Users are provided with a login account to the Lenus platform which is accessed via the clinical dashboard application. For each Health Board, a 'superuser' will be nominated by the Board. The superuser account will be created by Storm. The superuser account is created with a fixed set of privileges, which is the set of information search, view, update privileges that are accorded to all clinical users, with the addition of the capability to add or remove clinical users for their own Health Board domain only. Additional clinical users will be provisioned (and removed from the system when required) by the superuser. For all non-superuser accounts, the privileges are granted the same: there is only one 'profile', with the exception that clinical users are able to access only the patient information from their own Health Board. There is a STT SSP. NSS also have an Access Control Policy V1.2. **PHS** have an equivalent or similar Access Control Policy. **Health Boards** have equivalent or similar policies and procedures. **Storm ID** - The solution has database audit controls in place which audit database events

Type of Control – examples	Description
	and queries. .
System auditing functionality and procedures	NSS Information Security Policy V1.5 Section 6 – Responsibilities – page 6-7. All NSS staff work within the NSS Confidentiality Guidelines and should not be accessing information they do not require for work purposes. All NSS staff also follow NSS Incident Reporting procedures and our systems are auditable. Storm ID - The solution has database audit controls in place which audit database events and queries for the SQL database within the solution. The audit logs are stored in Azure storage. Storm ID IT manager has responsibility for auditing system access and notifying of, and/or acting upon suspicious or unusual activity for Storm ID employees. Health Boards - Have similar policies to ensure they comply with their own legal obligations.
Operating system controls such as vulnerability scanning and anti-virus software	**Storm ID** application testing includes: · Functional testing · Regression testing · Browser and device testing · Exploratory Testing · Performance testing · Security scanning testing · Security Penetration testing The solution is cloud-based, so security updates are part of the service provided. Storm ID also use security and vulnerability scanners throughout the product life cycle to actively seek out and fix vulnerabilities in the system such as out of date software versions. Pen tests have been carried out and the platform is assured. A website vulnerability scanner was used throughout the product life cycle on a scheduled basis. **NDP** - Security Penetration testing on each major release of platform. Automated scanning of the application as part of every deployment. NES policies and procedures. **Azure** – Pen tests have been carried out and the platform is assured. A website vulnerability scanner was used throughout the product life cycle on a scheduled basis.

Type of Control – examples	Description
	NSS Information Security Policy V1.5 Section 5 - Information Security Policy Principles - page 5-6; Section 6 – NSS Responsibilities – page 6-7.
Network security such as firewalls and penetration testing	The solution is cloud-based, so adheres to cloud security principles.
Encryption of special category personal data	All information assets are encrypted at rest and in transit.
Cyber Essentials compliance(if applicable)	NSS are working towards accreditation for Cyber Essentials. Storm ID is Cyber Essentials Plus certified. The solution adheres to the five technical controls of Cyber Essentials: · Secure your Internet connection · Secure your devices and software · Control access to your data and services · Protect from viruses and other malware · Keep your devices and software up to date
System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available)	There is an SSP for Ensemble and the Corporate Data Warehouse (CDW). There is an SSP for ECOSS being developed, however, penetration testing has been completed and the risks highlighted have been actioned. There is a SPP for the Simple Tracing Tool (STT) and a simple tracing tools set up pack with guidance for staff using the system. Staff will be fully trained and will use scripts whilst using the system. There is a SSP for the NDP.
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 Information Security Management System (ISMS) and security which is consistent with the standard. Microsoft Azure has ISO27001 accreditation.

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.

Consultation took place with the Data Protection Officers for:
- NHS National Services Scotland
- Public Health Scotland
- NHSScotland Territorial Boards
- NHS National Education Scotland

The Scottish Government and the NSS Chief Clinical Informatics Officer 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. ECOSS SSP being developed, however, penetration testing has been completed and risks actioned. • 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 letter 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

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
2. Failure of system security leading to data breach.	3.22 3.24 3.25 3.26 3.27 3.28	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. • Territorial Boards deriving assurance from national process/system provider.	**LOW**	Public Health Scotland; National Services Scotland	19 June 2020
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	3.8	Likely	Moderate	**MODERATE**	• National privacy notice published. • Additional information published by Territorial Boards. • Widespread public information	**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
(transparency).					programme from Scottish Government.		Medical Directors/SIROs , Territorial Boards	
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.	**VERY LOW**	Public Health Scotland; National	19 June 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
				MODERATE	• Data provided by individuals in respect of their contacts used in good faith. • Process to correct data available from all parties. • Exceptions process is in place to assist with both data quality and CHI matching	VERY LOW	Services Scotland; Medical Directors/SIROs, Territorial Boards	
7. Individual known to member of tracing staff – inappropriate disclosure.	3.22 3.23	Possible	Moderate	MODERATE	• Tracers subject to contractual/confidential controls. • Training to include how to respond to this issue.	VERY LOW	Public Health Scotland; National Services Scotland; Medical Directors/SIROs, Territorial Boards	19 June 2020
8. Inappropriate use of personal contact details in breach of PECR.	3.22 3.23 3.24	Unlikely	Minor	LOW	• Personal contact details provided by tested person for a clear purpose. • Contacts are 'service messages' concerning the Test and Protect	VERY 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
					process and are not being used for promotion/marketing.		Medical Directors/SIROs, Territorial Boards	
9. Profiling on the basis of special category data leading to fully automated decision making in breach of Article 22, GDPR.	3.16	Unlikely	Minor	LOW	• No fully automated profiling – Article 22 does not therefore apply. • Expanded uses such as profiling and/ or automated decision-making could not begin until a full DPIA and information security risk assessment etc. was completed	VERY LOW	Public Health Scotland; National Services Scotland; Medical Directors/SIROs, Territorial Boards	19 June 2020
10. Inadvertent joint controller arrangement established without Article 26 GDPR agreement	3.18	Unlikely	Minor	LOW	• SG Directive letter 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
11. Eavesdropping or disclosure of information due to homeworking. Also	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.	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
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.					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. • The appointment processes at national or Territorial Board level (confidentiality agreements and/or contractual control). • Training to be provided to all users. • Sponsoring Special or Territorial Board to assure own processes in respect of devices/setting etc. • In Tune – a mobile device management service, will be used to minimise the potential for screenshots to be taken • Homeworking policy will be in place.			
12. Inappropriate access to information due to	3.22 3.23	Possible	Major	**MODERATE**	• Staff will have a username and password that they should not	**LOW**	National Services	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
others living in a household.	3.24				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. 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. • All user actions are recorded as part of the service of the application audit logs. • Homeworking Policy will be in place		Scotland	
13. Availability Breach	3.22 3.24 3.25 3.26 3.27	Possible	Major	**MODERATE**	• At any one time, three database replicas are running—one primary replica and two or more secondary replicas. If the hardware fails on the primary replica, then the failure is detected and fails over to the secondary replica. In case of a	**LOW**	National Services Scotland	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
	3.28				physical loss of a replica, a new replica is automatically created. So, there are always at minimum two physical, consistent copies of our customers' data in the datacentre. Application servers are also automatically replicated to protect customers of failure of an individual server.			
14. Contacting the wrong person	3.22 3.23 3.24	Possible	Moderate	**MODERATE**	• Data as recorded by Special and Territorial Boards to be used for main records. • No personal data released to the patient. • Staff training. • Privacy sensitive script being use to verify identity of patient.	**VERY LOW**	National Services Scotland; Territorial Boards; Health Boards Contact Tracers	3rd July 20
15. Personal data provided to the traced patient without consent of the	3.22 3.23 3.24	Unlikely	Moderate	**LOW**	• Training to include how to respond to this issue. • Contact tracer scripts will reinforce that no personal data should be released unless the positive patient	**LOW**	National Services Scotland; Health Boards Contact Tracers	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
positive patient					has explicitly said they would like their details released.			
16. Identity of infected person implicitly revealed as they have only been in contact with one person.	3.22 3.23 3.24	Possible	Moderate	**MODERATE**	• Contact Tracers will be trained to not give any information, however, if the person has only been in contact with one person, this is a risk that will be explained to index cases, so they can understand that it may not always be possible in these cases to hide their identity due to circumstances.	**LOW**	National Services Scotland	3rd July 20
17. 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
18. 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	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.	**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
	3.7 3.20 3.25			**MODERATE**	• Any further purposes would be subject to a rapid assessment and DPIA.	**LOW**		
19. 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 • There will be a research value for Covid 19 data, all such requests will be subject to further approvals and independent oversight.	**LOW**	National Services Scotland; Public Health Scotland; SIRO's	3rd July 20
20. 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	**LOW**	National Services Scotland; Public	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					• 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.		Health Scotland; SIRO's	
21. 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
22. There is a risk that excessive personal data is collected on an individual.	3.1 3.2 3.7	Unlikely	Minor	**LOW**	• Datasets have been developed to only collect the information necessary. Datasets provided within the DPIA. • Tracers will only collect the minimum information in order to successfully contact anyone the patient may have been in contact with.	**VERY LOW**	National Services Scotland; Public Health Scotland	3rd July 20
23. 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	**MODERATE**	• An exceptions process has been developed to identify any mismatches • The National Integration Hub (Ensemble) performs a CHI look up using embedded algorithm within the system which is carried out automatically upon receipt of data.	**MODERATE**	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
					• 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. • Any unmatched records, known as 'exceptions', will be flagged for further processing.			
24. Relevant or new data processors may not all have adequate data processing agreements in place	3.20	Unlikely	Moderate	**LOW**	• Contracts and Data Processing Agreements are in place with known relevant processors. • Any new processors will be included in an updated DPIA and will have a specific DPA put in place, prior to processing. • The contracts in place with current suppliers are GDPR compliant	**VERY LOW**	National Services Scotland; Public Health Scotland; SIRO's	3rd July 20
25. 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 3.28 3.31	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

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
	3.32 3.33 3.34 3.35 3.36 3.37 3.38			**MODERATE**		**LOW**		
26. Personal data for additional phases of this process, may not be encrypted both/either in transit or at rest	3.35	Unlikely	Major	**MODERATE**	• All information assets within the SaaS solutions are encrypted at rest and in transit • FIPS 140-2 8x8 utilises Vendor provided encryption solutions which comply with the US FIPS 140-2 standards as a minimum. • Any future additional processes will ensure that full encryption compliance is both understood and in place and reflected in any relevant SSP.	**LOW**	National Services Scotland; Public Health Scotland; SIRO's; Processors	3rd July 20
27. Lower than expected public trust due to scam/fake calls,	3.8	Possible	Major	**MODERATE**	• Additional information published by Territorial Boards.	**LOW**	National Services	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
could lead to low participation for contact tracing					• Widespread public information programme from Scottish Government. • Updated privacy notices from Scottish Government.		Scotland; Public Health Scotland; Scottish Government.	
28. Contact centre staff may enter personal details incorrectly	3.22 3.23 3.24	Possible	Major	**MODERATE**	• Training and guidance for all staff using systems and personal data. • Data can be confirmed with patients if necessary.	**LOW**	National Services Scotland; Public Health Scotland;	3rd July 20
29. Contacting patients by telephone may be seen by some as an invasion of privacy	3.8 3.23	Possible	Major	**MODERATE**	• Contact tracing is the process of identifying, assessing, and managing people who have been exposed to a disease to prevent onward transmission. When systematically applied, contact tracing will break the chains of transmission of COVID-19 and is an essential public health tool for controlling the virus. • Approach discussed and agreed with a range of stakeholders including the ICO. • Scripts should include statement of	**VERY 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
					re-assurances as to reasons this level of data collection is necessary • Scripts should include re-assurance around the security of data being collected			
30. 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	**MODERATE**	• Review policies regularly	**LOW**	National Services Scotland; Public Health Scotland;	8th July 2020

17. Review and Sign-Off

Role	Advice/ Action/ Sign-Off	Date
Data Protection Officer (DPO) Advice	Comments provided by both NSS and PHS DPOs and advice given prior to SARB approval on 18 August 2020	
Information Security Officer Advice (questions 11 and 12)		
Others, if necessary e.g. Caldicott Guardian, Senior Information Risk Owner (SIRO)	Deputy SIRO review throughout drafting process	
DPO opinion on whether residual risks need prior notification to the ICO	ICO consulted as part of the creation of DPIA	
Information Asset Owner(s) (IAO(s)) Sign Off	Approved by SARB on 18 August 2020	

18. **Recommended Review Date:**   STT has been superseded by CMS and is no longer part of the pandemic response. This DPIA will not be reviewed unless that position changes.

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