Data Protection Impact Assessment (DPIA) Questionnaire for

Case Management System

23 July 2020

DOCUMENT CONTROL SHEET

Key Information

Title	Case Management System (CMS)
Date Published/ Issued	23 July 2020
Date Effective From	23 July 2020
Version/ Issue Number	V1.0
Document Type	Data Protection Impact Assessment
Document Status	Approved by Security and Architecture Review Board on 23 July 2020
Author	NHS National Services Scotland
Owner	Deryck Mitchelson, Director Digital and Security
Approvers	Security and Architecture Review Board
Contact	
File Name	

Revision History

Version	Date	Summary of Changes
		See section 14
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 (comments from SARB which are incorporated into this version)

Version	Date	Name	Designation
V0.3 (renamed v1.0)	23/07/2020	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	No

		YES/NO
	Excludes: Processing with little or no effect on people	
2.	The work involves carrying out ***large scale*** processing of any of the ***special categories*** of personal data, or of ***personal data relating to criminal convictions and offences.*** 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	Yes
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.	Yes
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	No

		YES/NO
	public area that people passing by cannot avoid.	

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.**

As part of Covid-19 'Test, Trace, Isolate, Support' (TTIS), NSS have been asked by the Scottish Government to provide a system for a national contact tracing service for Covid-19. The Software as a Service (SaaS) capability is being provided to contact tracers to use the provider's application running on a cloud infrastructure.

The delivery model is hosted application management, with NSS hosting software for contact tracers and delivered over the internet. This document uses the Software as a Service (SaaS) security principles to provide a risk assessment of the system that we are providing.

https://www.ncsc.gov.uk/collection/saas-security/saas-security-principles

The simple tracing tool has been used to this point, but after some consideration and to better provide with future development, a decision was made to develop a tool that would be hosted and secured in our own azure environment.

It is considered proportionate as it allows for sufficient data to be collected and used at the correct points, and for it to be secured and shared appropriately for the provision of contact tracing and provision of care where needed. while also allowing for compliance to user rights (where applicable) and therefore meeting 'privacy by design' principles.

The collection of the data is necessary to:
1) To have access to the contact details of the data subject in a structured way in order to provide guidance and support
2) To provide support necessary to prevent infection and the spread of infection such as health education and information about support services
3) To keep individuals and members of the public safe during a public health emergency
4) To provide performance aggregate statistics in relation to numbers of contacts made, numbers of unsuccessful contacts, demographic characteristics of contacts, workload management statistics, etc
5) To provide data that can inform research into the effectiveness of contact tracing
6) To comply with the instructions from Scottish ministers in respect of protecting the health of the population.

Case Management Service (CMS) will replace the simple tracing tool and will facilitate, as part of Covid-19 and beyond, a well-established public health intervention methodology called "contact tracing". Contact tracing will be used to identify the close contacts of those cases who may have had the disease transmitted to them. These close contacts will then be asked to self-isolate so that, if they do develop the disease, there is less risk that of transmission to others. The contact tracers will use the CMS to enter contact tracing information for those patients with positive results, they will also view the submitted contacts and their relative priority level to enable targeted phone-based interviews to be arranged.

The case management service (CMS) leverages existing platforms used within NHS NSS, these tools are cloud based SaaS' (Software as a service) namely ServiceNow Customer

Service Management Module and also a new system called 8x8 Virtual Call Centre (VCC) and Virtual Office (VO). Both systems are integrated to make up the overall CMS solution.

The solution is driven by the daily lab results data feeds (3hrly) from the Electronic Communication of Surveillance in Scotland ('ECOSS') system which is the established core NHS Scotland service for disseminating laboratory test results.

MESH daily feeds (1/2 hrly) contain UK test data results.

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 of CMS 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 principal technical components and the virology data feed are all pre-existing technologies and services used in NHS Scotland, and the practice of using SMS and email for outbound messaging to patients is also established in other services in NHS Scotland.

NHS National Services Scotland (NSS) and Public Health Scotland (PHS) will both be controllers of the Case Management System, as both are involved in the definition of fields and linkages to other systems, as well as deciding on methods and how data will be used for reporting.

The service will be deployed in the territorial NHS Health Boards, who will be Data Controllers for all data pertaining to their patients. per their contribution to the Test and Protect process and where data is recorded in their systems.

Territorial Boards will be provided with access to the CMS to facilitate in-region contact tracing for more complex cases that cannot be managed by the contract tracing team. Access to CMS will be via Service Now.

The integration of the 8x8 telephony service with CMS will allow calls to be made to individuals directly from the system, removing the need for additional devices and reducing the potential footprint of personal data.

The "8x8 Telephony" systems, Virtual Contact Centre (VCC) and Virtual Office (VO) provide the telephony capability for Contact Tracers to communicate with patients and citizens (non-patients) who are potentially at risk of suspected disease through contact with someone who may have been at risk of suspected disease.

8x8 have provided a document detailing the data handling, types of data and encryption process by 8x8.

Communication between contact Tracers and patients or citizens is two-way, through use of outbound and inbound calls.

To facilitate for the sharing of data between boards, it has been necessary to put in place a data sharing accord. This can be found using the link below.

https://www.informationgovernance.scot.nhs.uk/wp-content/uploads/2020/06/2020-06-17-Intra-NHS-Scotland-Sharing-Accord-v2.0.pdf

The official instruction can be found here:
https://www.informationgovernance.scot.nhs.uk/wpcontent/uploads/2020/06/DL-Intra-NHS-Scotland-Information-Sharing-Accord-2020.pdf

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 Email Phone number DoB Age	CHI number Health data – test results. Ethnicity	Provided by patient, ECOSS, Health Boards, 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 public interest or in the exercise of official authority vested in the controller.	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) 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.
Covid-19 is an international pandemic which has been deemed so by the world health organisation. This holds a serious threat to life for index cases and any contacts who may	

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

have been infected as a result of contact with index cases. It is therefore vital and has been mandated by the Scottish Government that organisations need to work together and share information appropriately to alleviate and minimise this threat, in order to prevent further infection and possible death to citizens.

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 (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

Concerning 9(2)(i), per Schedule 1, Part 1 paragraph 3 DPA 2018, processing is carried out under the responsibility of the Medical Directors of the special and territorial health Boards.

The necessity test for these conditions are met due to the processing being necessary:
1) To have access to the contact details of the data subject in a structured way in order to provide guidance and support
2) To provide support necessary to prevent infection and the spread of infection such as health education and information about support services
3) To keep individuals and members of the public safe during a public health emergency
4) To provide performance aggregate statistics in relation to numbers of contacts made, numbers of unsuccessful contacts, demographic characteristics of contacts, workload management statistics, etc
5) To provide data that can inform research into the effectiveness of contact tracing
6) To comply with the instructions from Scottish ministers in respect of protecting the health of the population.

For NSS they are also operating as per 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 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). PHS is also an official statistics producer and has a legal a gateway for producing official statistics on any matter as set out in The Official Statistics (Scotland) Order 2008, The Official Statistics (Scotland) Amendment Order 2019 and the Statistics and Registration Service Act 2007. PHS will produce statistics on the activity captured within the case management service in accordance with GDPR Article 89(1).

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 CMS is new, 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 hitherto be practicable.

From a contact tracing process perspective, the CMS 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 CMS described in this document is specific to Covid-19 tests.

T**he service operates as follows:**
(a) The existing daily export file containing virology lab results is sent by the 'ECOSS' system via the NHS NSS National Integration Hub (NIH), where the CHI matching is done then on to Service Now. The UK Data results are sent to NIH and then on to Service Now
(b) Any unmatched CHI will be part of an exceptions process.
(c) Contact Tracers will then access relevant results and will use data when using 8x8 to contact both index cases and contacts. Data retrieved by tracers will be added to the Service Now case.
(d) Contacts will be added to service now if we do not have a current record for them and all relevant details will be stored there.
(e)Positive cases will then be picked up by health workers through Service Now, to then provide appropriate health care.
(f) Data will be stored in the corporate data warehouse (CDW) for future research and reporting purposes.

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

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 privacy notice for Test, Trace, Isolate and Support can be found here:
https://www.informationgovernance.scot.nhs.uk/use-of-your-data-for-track-trace-isolate-tti/

SG Covid 19 data general privacy notice can be found here:
https://www.informationgovernance.scot.nhs.uk/covid-19-privacy-statement/

All territorial health boards
Have their own privacy notices which can be found on their websites.

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

The PHS privacy notice can be found here: https://www.publichealthscotland.scot/our-privacy-notice/

In relation to the use of **8x8** for recording calls, a privacy notice is given by way of an agreed script being read out by contact tracers. Calls are being recorded for both quality and training purposes.

NOTE: It is the responsibility of each board to update their privacy notice, to reflect any 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 right of access will be done using the subject access processes currently in place. Patients would normally contact their own health board in the first instance. However, this work will not affect an individual's right to access their data which may be held by any other organisation, who may have responsibility as a data controller e.g. NSS or PHS via their Data Protection Officer whose contact details should be in their respective Privacy Notice.

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

Service Now has a process in place that will allow requests to be lodged and processed. This will include access to call recordings held either by 8x8 or in the corporate data warehouse. Service Now has the capability to comply with this right when requested to do so. A robust procedure for this has been developed.

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:

It is anticipated that information held within systems should be accurate. However, if it's agreed that a patient's data is inaccurate, the information will be rectified as quickly as possible, but no later than one month, or within two months where the

request is complex. Information on the right to rectification is available on all health boards privacy notice. which can be found on the websites.

Where this data is processed elsewhere, it is the responsibility for the controlling board to advise others of any rectification to ensure the integrity of the data.

Requests will be considered on a case by case basis.

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

Service Now has a process in place that will allow requests to be lodged and processed. This will include access to call recordings held either by 8x8 or in the corporate data warehouse. Service Now has the capability to comply with this right when requested to do so. A robust procedure for this has been developed.

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, compelling 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 comply with this right when requested to do so. This will also include any data that may be held by either 8x8 or in the Corporate Data Warehouse. A robust procedure for this has been developed.

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 the capability to comply with this right when requested to do so. This will also include any data that may be held by either 8x8 or in the Corporate Data Warehouse. A robust procedure for this has been developed.

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 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).

Right to erasure requests are dealt with on a case by case basis.

Service Now has the capability to comply with this right when requested to do so. This will also include any data that may be held by either 8x8 or in the Corporate Data Warehouse. A robust procedure for this has been developed.

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

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 kept by PHS for 7 years after the threat of Covid-19 to the life of Scottish residents is declared over. Permission to use data for research is normally given by the Public Benefit and Privacy Panel for Health and Social Care (HSC-PBPP). This comprises patient representatives, lay people, Caldicott Guardians of NHS boards, IG practitioners and data specialists. Permission will therefore be sought when required.to facilitate historical research and statistical reporting in the public interest. All statistical and research outputs will meet the requirements of Article 89(1) in the GDPR and Section 19 of DPA2018.

8x8 Service will keep call recordings for 10 days at which point it will be securely transferred via Secure File Transfer Protocol (SFTP) to the Corporate Data Warehouse (CDW) to ensure we are able to comply with retention requirements.

8. Who will have access to the personal data?

Data is input to the case management system by contact staff who will all be employees of NHS NSS and will be bound by contracts and confidentiality undertakings. They will also be trained in information governance prior to being able to access any personal data.

Health board staff will also be able to access the CMS in order to identify index cases for whom they will then provide appropriate health care services. There will also be some in region contact tracing done by health board staff, particularly for complex cases passed over by contact tracers. PHS who are also controllers will have access to the system through their authorised health surveillance staff who will be monitoring this pandemic and the services being provided to deal with it. PHS will also be responsible for aggregating any reports to provide statistical analysis and reports which would have undergone statistical disclosure assessment.

Public Health Scotland - Data Controller. The service is part of the HPS Covid-19 response measures, ensuring patients who test negative 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.

NHS Scotland Boards as data controllers for data pertaining to their own patients. Territorial Health Boards whose contact tracing 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).
- View and update information relating to index (C19-positive) case and their contacts

The territorial Boards using this service and providing additional data feeds are also Data Controllers for the data pertaining to their own patients, or joint data controllers where determining the manner and purpose of processing with NSS following transfer. Participating Boards will also provide first line support so may access the service to assess problems and alert second line support.

NHS National Services Scotland - NSS, as a Data Controller will operate the service on behalf of NHS Scotland Boards. NSS will be a data controller, due to the infrastructure it provides within NSS and to PHS and is uniquely placed to coordinate this work. NSS are facilitating by hosting data, determining data fields required with PHS, how data will be collected, linked and transferred between relevant systems and processes.

This means that any staff operating the following systems, may have access to limited data pertinent to their role and function only. All are NHS employees who are bound by contracts and organisational policies and expected to all be trained in Information Governance via Learn Pro (the internal learning and development system).

Systems where access may be obtained include: National Integration Hub (NIH). The NIH receives incoming data feeds from the PHS ECOSS service. This contains patient, Health Board, and laboratory test result information that is processed and filtered by the NIH. Service Now is the customer service module that is used to integrate with the 8x8 telephony system. 8x8 is an external third party company providing the virtual office telephony service. They will only have access to users details for login and authentication purposes, and limited demographic details for patient contact. They will also record and host calls for 10 days at which point recordings will be transferred to an NSS secure host site, for retention purposes.

A Data Processor Agreement (DPA) has been produced for 8x8, but they will only have access to minimal contact details to facilitate for their system, in order to provide contact tracers to the numbers to contact both index cases and relevant contacts. It is worth noting that the contact tracers connect to Service Now and login to the 8x8 telephony module via this route and that no personal data is stored on contract tracers devices. All data is hosted on secure cloud based environments with all appropriate controls as defined by the relevant system security policies (SSP's).

Support staff for any system, be it an existing NHS one (ECOSS) or a new one (8x8) will only have access to data related to system functions and data for support requirements, for example, user authentication. Support staff will not have access to personally identifiable patient data, unless this is part of an agreed function for which they have some responsibility. Such functions should be detailed in a Data Processing Agreement or Data Sharing Agreement (if appropriate).

All systems being utilised have role based access controls in place and appropriate auditing functionality for activities undertaken.

Contact tracers do not have access to all of the Service Now functionality, but are limited to only cases that they are passed via the automated queue for calls.

The majority of access will be for health and social care purposes and is therefore covered under (Schedule 1, Part 1, paragraph 2(1) and 2(2)(d and f) DPA 2018)

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.**

Data will not be shared out with those already specified in this document under question 3.17 Who will access the data.

As also stated earlier any outputs from CMS will all be aggregated anonymised reports used for research and statistical reporting.

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).**

8x8: 8x8 are a SaaS company being used for the following;
8x8 Virtual Contact Centre and associated support service, solutions proposals and costs were provided and are marked as confidential. A Data Processor Agreement is being considered and legal advice is being sought as to whether this is required given standard contractual terms.
8x8 - Telephony Service which meets Cyber Essentials Plus certification. The "8x8 Telephony" systems (VCC and VO) provide the telephony capability for Contact Tracers to communicate with patients and citizens (non-patients) who are potentially at risk of suspected disease through contact with someone who may have been at risk of suspected disease. Communication between contact Tracers and patients or citizens is two-way, through use of outbound and inbound calls. The VCC contains the Agent Console and Supervisor Console. Selection criteria, processing instructions and contracts are marked as confidential, but are available for confidential viewing where necessary.

Microsoft provide the following
Microsoft Azure NHS Scotland Azure Environment.
Microsoft Azure Cloud Services are used to host the authentication services, this will only hold login details for users of CMS.
Microsoft Azure has completed Level 2 of the NHS IG Toolkit.
(https://download.microsoft.com/download/7/F/6/7F6EBDDE-F3EF-4225-ACDAADCD851430C4/NHS_IG-Compliance.pdf)"

Service Now
Service now is SaaS platform used to provide the CMS functionality and will therefore host all the contact tracing data. A full DPIA for this service will be attached when finalised.

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)	All **health boards** have their own policies and procedures. They can be obtained information governance leads within each board. Policies will be similar to those detailed below for National Services Scotland. **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 • NSS Homeworking Policy (TBD) • Bring Your Own Device Policy (TBD) **Procedures** • Destruction Process for hard drives and mobile phones – CST • NSS Data Cleansing Guidelines • Decommissioning and destruction of IT desktop devices Case Management System SSP 8x8 have their own security policies covered under their Security Statement paper, currently marked as confidential. This has been reviewed by security personnel within NHS NSS and is being used to inform the System Security Policy for this process. There is also an SSP for NIH (Ensemble) and Service Now.
Staff training	All NHS Board staff are required to complete mandatory Information Governance training. All parties have mandatory/statutory Data Protection/Information Governance training in place which staff undertake on a regular basis. This is normally an online module and a test via learn pro or Turas (Training system). NHS Scotland Boards also have their own data protection and confidentiality policies and guidelines.

Type of Control – examples	Description
	NSS also have Confidentiality Guidelines V1.1a. Contact tracers will all be trained to this level as a minimum, prior to be given access to any system utilising personally identifiable data. There is SSPs for 8x8, NIH Ensemble and Service Now.
Adverse event reporting and management	NSS and PHS have an Adverse Events Management Policy and staff can report any adverse events via our adverse events portal. NHS Scotland Territorial boards also have systems including Qpulse and Datix for their adverse event management processing. NSS have an adverse events policy. There is SSPs for 8x8, NIH Ensemble and Service Now. As NIH and Service Now are managed by NSS, current NSS adverse event reporting will be used appropriately.
Physical access and authorisation controls	All NHS Scotland boards will have internal policies requiring controls to be in place appropriately. They can be obtained by contacting an information governance or data protection lead within that board. NHS policies relevant to this type of control include; **NSS 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 a **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** There is SSPs for 8x8, NIH Ensemble and Service Now.
Environmental controls	**Microsoft Azure** is our cloud based service which holds the active directory of users to be authenticated to use CMS.

Type of Control – examples	Description
	Microsoft Azure has completed Level 2 of the NHS IG Toolkit. System controls are detailed in the SSPs. There are SSPs for 8x8, NIH Ensemble and Service Now.
Information asset management including management of backups and asset disposal	As data controllers, all boards have their own information asset register. It is the boards responsibility to keep this up to date and ensure information is held in line with the Scottish Government Records Management Health and Social Care Code of Practice 2020. NSS also has the Document Storage, Retention and Disposal Policy v7.3. Other boards may have similar policies and procedures and should be available from appropriate information governance and data protection leads for each board. NSS also have the following procedures and guidelines: • Destruction Process for hard drives and mobile phones – CST • NSS Data Cleansing Guidelines • Decommissioning and destruction of IT desktop devices Backup and disposal are detailed in the SSPs. There are SSPs for 8x8, NIH Ensemble and Service Now.
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. Service Now - Regular, automated tests are run to ensure the quality of backups. Any failures are reported for remediation within ServiceNow. For the provision of Disaster Recovery, instant data replication is between Data Centres. This data transaction is secured by encryption 8x8 have disaster recovery built into their service.

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

Type of Control – examples	Description
System access levels and user authentication controls	All boards will have their own policies regarding system access levels and user authentication controls. They will be similar to the one detailed below for NSS. Regarding this case management system being rolled out as a national system, we would look to adhere to the policy in place for NSS detailed below. **NSS Access Control Policy v1.1 Physical access** • Physical Access shall only be granted on the authority of the Information Asset Owner and shall be applied on a strict 'Need to Know' basis. • All NHS information assets shall be physically protected in accordance with their data and security classification. • Information Asset Owners shall implement physical security measures in order to control Physical Access to information assets, in addition to any physical access controls for the buildings in which they are located. • The Information Asset Owner should keep an access log (date/time/name/reason) of service user access to information assets, for audit purposes and in line with their service requirement and the service record retention requirements. • Any unauthorised access shall be reported as an information governance adverse event. **Network access** • All staff and contractors shall be given network access in accordance with the requirements for access defined by their roles. • Anyone who accesses NSS networks remotely shall only be authenticated using the approved remote access authentication mechanism. • Diagnostic and configuration ports shall only be enabled for specified business reasons. All other ports shall be disabled or removed. • Risk assessment shall be conducted by NSS to determine the requirements for the segregation of networks. • Segregation of networks shall be implemented as determined by the results of the risk assessment. • Network administrators shall group together information services, users and information systems as appropriate to achieve the required segregation on networks. • Network routing controls shall be implemented to support the access control policy. **Application and information access** • Users shall only be granted access to those application functions required to carry out their roles. • Users shall only be granted access to information in applications in accordance with

Type of Control – examples	Description
	business access requirements and policy. • Systems should be physically or logically isolated in order to meet the requirements of restricted access to authorised personnel. System access controls are detailed in the SSPs.
System auditing functionality and procedures	Within CMS there is an audit of recent events at the bottom of the page for Index Cases. Service Now also has auditing capabilities and a reporting infrastructure for building and utilising bespoke reports for auditing.
Operating system controls such as vulnerability scanning and anti-virus software	Systems will have anti-virus software and vulnerability scanning tools in place. Controls are detailed in the SSPs. This control is also underpinned by policies for all boards, similar to those outlined for NSS below: **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	PEN testing is regularly performed on ServiceNow and 8x8 SaaS systems. Tests are performed by a third party on an annual basis, this along with the daily vulnerability scanning helps identify risks and remediation that increase security of the managed service. Network security is detailed in the SSP's.
Encryption of special category personal data	Data is encrypted at both rest and in transit. NSS also underpin encryption via NSS Encryption Policy V1.1. NSS information should be protected on NSS IT systems, portable IT devices, mobile data storage media, secure file transfer and email services and for user remote access solutions from unauthorised access through use of approved encryption solutions. Approved cryptographic algorithm shall meet industry standards such as FIPS 197. The use of software that does not benefit from independent security evaluation or does not meet industry standards such as ISO/IEC 15408 and FIPS 140-2 shall not be implemented.
Cyber Essentials compliance (if applicable)	NSS are currently working towards Cyber Essentials accreditation. 8x8 meet Cyber Essentials Plus.
System Security Policy (SSP) and Standard	There is an SSP and Operating procedures for

Type of Control – examples	Description
Operating Procedures(SOPs) (if applicable/ when available)	the Case Management Service (CMS) There are SSPs for 8x8, Service now and NIH Ensemble. A SSP for ECOSS is being developed.
Details of ISO27001/02 accreditation (if applicable)	Microsoft Azure has ISO27001 accreditation. 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. Whilst we at NSS are not accredited to this standard, we operate in compliance with SG IS policy which is designed to be consistent with this ISO standard

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.**
    Consultation for this CMS/8x8 DPIA has been sought from:

    The Data Protection Officers and Information Governance leads for:
    - NHS National Services Scotland
    - Public Health Scotland
    - NHSScotland Territorial Boards
    - NHS National Education Scotland

    Others consulted include:
    - Scottish Government representatives
    - ICO Representatives

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

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.	3.24	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 letter (22nd 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.	3.21 3.23 3.24 3.25	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
	3.26 3.27				• Territorial Boards deriving assurance from national process/system provider.			
3. Failure of system leading to data loss.	3.21 3.23 3.24 3.25 3.26 3.27	Possible	Major	**MODERATE**	• CMS is built using SaaS ServiceNow and 8x8, so software hosted in the cloud that NSS simply consume. These SaaS platforms are globally highly available; they have a 99.9% uptime. • 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	3.8	Likely	Moderate	**MODERATE**	• National privacy notice published. • Additional information published by Territorial Boards. • Widespread public information	**LOW**	Public Health Scotland; National Services	19 June 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
processed and why (transparency).					programme from Scottish Government.		Scotland; 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	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	3.11	Possible	Moderate	**MODERATE**	• Data as recorded by Special and Territorial Boards to be used for	**VERY LOW**	Public Health Scotland;	19 June 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
used in the process.					main records. • 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		National Services Scotland; Medical Directors/SIROs, Territorial Boards	
7. Data security – There is a risk of a data security breach by tracing staff due to the challenging circumstances in which their recruitment and training has taken place	3.21 3.22	Possible	Moderate	**MODERATE**	• 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. • Support in place during calls where requested or required	**MODERATE**	Public Health Scotland; National Services Scotland; Medical Directors/SIROs, Territorial Boards	19 June 2020
8. Individual known to member of tracing staff – inappropriate	3.21 3.22	Possible	Moderate	**MODERATE**	• Tracers subject to contractual/confidential controls.	**VERY LOW**	Public Health Scotland; National	19 June 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
disclosure.					• Training to include how to respond to this issue.		Services Scotland; Medical Directors/SIROs, Territorial Boards	
9. Inappropriate use of personal contact details in breach of PECR.	3.21 3.22 3.23	Unlikely	Minor	**LOW**	• Personal contact details provided by tested person for a clear purpose. • Contacts are 'service messages' concerning the Test and Protect process and are not being used for promotion/marketing.	**VERY LOW**	Public Health Scotland; National Services Scotland; Medical Directors/SIROs, Territorial Boards	19 June 2020
10. Profiling on the basis of special category data leading to fully automated decision making in breach of Article 22, GDPR.	1.1	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	19 June 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
							Boards	
11. Inadvertent joint controller arrangement established without Article 26 GDPR agreement	3.17	Unlikely	Minor	**LOW**	• SG Directive letter (22nd June 2020) establishes standards and rationale for inter-Board sharing via implementation of Information Sharing Accord.	**VERY LOW**	Scottish Government.	19 June 2020
12. Eavesdropping or disclosure of information due to homeworking. Also 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	3.21 3.22 3.23	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. • The appointment processes at national or Territorial Board level (confidentiality agreements and/or contractual control). • Training to be provided to all users.	**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
etc of patient details, thereby causing a data breach.					• 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 is in place.			
13. Unauthorised use of devices that do not meet scope of BYOD Policy. This risk will only be relevant when the BYOD is live. It is currently being developed.	3.21 3.22 3.23	Possible	Major	**MODERATE**	• This will be mitigated by providing NSS devices to the initial group of contact tracers. • A BYOD policy is being developed and will be explained thoroughly through training/guidance and advice to all staff using systems and services. • IT have been consulted on the minimum system requirements for any BYOD.	**LOW**	National Services Scotland	3rd July 20
14. Inappropriate access to information due to others living in a	3.21 3.22	Possible	Major	**MODERATE**	• Staff will have a username and password that they should not share with others.	**LOW**	National Services Scotland	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
household.	3.23				• They will have access to the minimum required data in order to complete their tasks. • Staff will receive training on 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 is in place			
15. Availability Breach	3.21 3.23 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, Azure SQL Database detects the failure and fails over to the secondary replica. In case of a physical loss of a replica, a new replica is	**LOW**	National Services Scotland	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					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.			
16. Contacting the wrong person	3.21 3.22 3.23	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 used to verify identity of patient.	**VERY LOW**	National Services Scotland	3rd July 20
17. Personal data provided to the traced patient without consent of the positive patient	3.21 3.22 3.23	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 has explicitly said they would like	**LOW**	National Services Scotland	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					their details released.			
18. Identity of infected person implicitly revealed as they have only been in contact with one person.	3.21 3.22 3.23	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. • Check to see if support advice is given in these circumstances.	**LOW**	National Services Scotland	3rd July 20
19. Systems can be at risk from human error at system supplier level (e.g. programming error)	3.11 3.19	Unlikely	Major	**MODERATE**	• Appropriate testing by supplier and users	**LOW**	National Services Scotland; Processors	3rd July 20
20. 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	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	**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
	3.6 3.7 3.19 3.24				purpose. • Any further purposes would be subject to a rapid assessment and DPIA.			
21. There is a risk that personal data is retained for longer than necessary.	3.16	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 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.	**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
					• There will be a research value for Covid 19 data, all such requests will be subject to further approvals and independent oversight.			
22. There is a risk that the personal data is no longer relevant.	3.16	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
23. There is a risk that personal data is passed to external organisations.	3.17 3.18	Unlikely	Major	**MODERATE**	• No data will be shared with organisations other than those listed within this DPIA.	**VERY LOW**	National Services Scotland; Public Health Scotland	3rd July 20
24. 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

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
25. 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 Community Health Index (CHI) look up using embedded algorithm within the system which is carried out automatically upon receipt of data. • 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.	**MODERATE**	National Services Scotland; Public Health Scotland; SIRO's	3rd July 20
26. Relevant or new data processors may not all have adequate data processing agreements in place	3.19	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
27. Lack of technical or organisational measures	3.21	Possible	Major	**MODERATE**	• Well established hosting arrangements testing in controlled environment	**LOW**	National Services	3rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
implemented to ensure appropriate security of the personal data	3.23 3.24 3.25 3.26 3.27 3.30 3.31 3.32 3.33 3.34 3.35 3.36 3.37				• Procedure for secure transfer of data is documented and followed • Backup in place for 8x8 data		Scotland; Public Health Scotland; SIRO's; Processors	
28. Personal data for additional phases of this process, may not be encrypted both/either in transit or at rest	3.34	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	**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
					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.		Processors	
29. Lower than expected public trust due to scam/fake calls, could lead to low participation for contact tracing	3.8	Possible	Major	**MODERATE**	• Additional information published by Territorial Boards. • Widespread public information programme from Scottish Government. • Updated privacy notices from Scottish Government.	**LOW**	National Services Scotland; Public Health Scotland; Scottish Government.	3rd July 20
30. Contact centre staff may enter personal details incorrectly	3.21 3.22 3.23	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
31. Contacting patients by telephone may be seen by some as an invasion of privacy	3.8 3.22	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	**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
					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 re-assurances as to reasons this level of data collection is necessary • Scripts should include re-assurance around the security of data being collected			
32. 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	3.21	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 23 July 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 23 July 2020	

18. Recommended Review Date: DPIA to be reviewed constantly throughout pandemic response period as a live document and thereafter every year.

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