



Data Protection Impact Assessment (DPIA) Questionnaire for

NATIONAL NOTIFICATION SYSTEM (NNS)

V1.0

18 August 2020

DOCUMENT CONTROL SHEET

Key Information

Title	National Notification System (NNS)
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 and DHI
Owner	NHS NSS
Approvers	Security and Architecture Review Board
Contact	
File Name	National Notification System (NNS) DPIA v0.1

Revision History

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

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. <u>Includes:</u> Profiling and predicting, especially when using aspects about people's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements Processing with effects on people such as exclusion or discrimination	No

		YES/NO
	<u>Excludes:</u> Processing with little or no effect on people	
2.	<p>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.</p> <p><u>Includes:</u></p> <ul style="list-style-type: none"> • 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 <p><u>To decide whether processing is large scale you must consider:</u></p> <ul style="list-style-type: none"> • 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.	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 <u>European Economic Area</u> .	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	

	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.

This DPIA is the 2nd of a set of 4 DPIAs which have been carried out to underpin the change in data processing arrangements made in our organisation, NHS National Services Scotland (NSS) as a result of the Scottish Government's response to the Covid-19 pandemic.

Covid-19 National Notifications Service

The Covid-19 National Notifications Service (NNS) is a new service being developed as part of the Digital Health and Care Institute's portfolio of responses to the current Covid-19 outbreak. Scottish Government are engaging with the public which includes television coverage and letters sent to all those considered potential high risk patients.

COVID-19 community testing services in Scotland are operating at maximum capacity in terms of testing patients and communicating results to tested patients within a forty-eight-hour period. A significant amount of time is spent in manual results lookup and contacting patients, and these activities have been identified as factors limiting testing capacity, leading to an increasing backlog of people waiting for test results.

The purpose of the Covid-19 National Notifications Service is to remove a significant burden of NHS effort spent manually notifying patients of Covid-19 test results using lists and telephones. Removing this task will free up capacity within the service, will allow it to carry out more tests per day and to focus valuable resources on managing patients who test positive.

The majority of test results are expected to continue to be 'negative', and therefore if patients could be notified of their results using an automatic service it would significantly reduce manual effort by NHS staff spent contacting patients.

The solution National Notification System was proposed by DHI to help Scotland cope with the demands being placed on the care services, however, NSS are now leading on this work and the NNS will notify patients that their test result is available to view via an online service.

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.

NSS and PHI will be a data controller. NSS and PHS are uniquely placed to coordinate this work. NSS are completing this DPIA as we are facilitating by hosting a lot of the data, determining how data will be collected, linked and transferred between relevant systems and processes.

CHI is matched on the following variables - Name, Date of Birth, Gender, Postcode. There is a CHI Exceptions process for any that do not match, where this is 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.

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	Health data (test results)	Data Subject, Health Board and ECOSS.

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

Legal condition(s) for <i>personal data</i> [see Guidance Notes]	Legal conditions for any <i>special categories of personal data</i> [see Guidance Notes]
	9(2)(i) - Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
<p>The Covid-19 National Notifications Service (NNS) is a new service, developed as part of the Digital Health and Care Institute’s portfolio of responses to the current Covid-19 outbreak.</p> <p>Article 6(1)e, Schedule 1, Part 1, paragraph 2(1) and 2(2)(d and f) DPA 2018</p> <p>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 and to collect and disseminate epidemiological data and participate in epidemiological investigations; and per section 37 and section 10(6) of the National Health Service (Scotland) Act 1978.</p> <p>Public Health Scotland are operating as per section 4 of the Public Health Scotland Order 2019 to protect public health including those specified in section 1 of the Public Health etc. (Scotland) Act 2008 (duty of Scottish Ministers to protect public health).</p> <p>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.</p> <p>These Article 9 exceptions rely on the following conditions from Part 1 of Schedule 1 of the Data Protection Act 2018:</p> <p>Article 9(2)(h) – Schedule 1, Part 1, paragraph 2(d) and 2 (f) DPA 2018 Article 9(2)(i)- Schedule 1, Part 1, paragraph 3 DPA 2018 Article 9(2)(j) – Schedule 1, Part 1, paragraph 4 DPA 2018</p> <p>The necessity test for these conditions are met due to the processing being necessary:</p> <ol style="list-style-type: none"> 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. <p>For NSS - National Services Scotland (“NSS”) is a Special Health Board operating as per</p>	

Legal condition(s) for <i>personal data</i> [see Guidance Notes]	Legal conditions for any <i>special categories of personal data</i> [see Guidance Notes]
<p>sections 2(f) and 2(j) of the National Health Service (Functions of the Common Services Agency) (Scotland) Order 20082 to provide information, advice and management services in support of the functions of Scottish Ministers, Health Boards and Special Health Boards and to collect and disseminate epidemiological data and participate in epidemiological investigations; and per section 37 and section 10(6) of the National Health Service (Scotland) Act 1978.</p> <p>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).</p> <p>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.</p>	

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

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

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

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

SG privacy notice for Covid 19 Testing can be found here: <https://www.informationgovernance.scot.nhs.uk/testing-for-covid19-privacy-information/>

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

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

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

The Public Health Scotland privacy notice can be found here: <https://www.publichealthscotland.scot/our-privacynotice/>

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 patient's personal information is inaccurate or incomplete we'll aim to amend the record(s) within one month, or within two months where the request is complex.

Service Now has 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 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. Who will have access to the personal data?

NHS National Services Scotland - NSS, as a Data Controller will operate the service on behalf of NHSScotland Boards. All systems being utilised have role based access controls in place and appropriate auditing functionality for activities undertaken.

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.

NHS Lothian, NHS Greater Glasgow & Clyde & all other 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 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.

StormID – provide the data platform providing patient information storage and processing. All systems being utilised have role based access controls in place and appropriate auditing is completed every six months, 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.

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

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

10. **Will the personal data be processed by a Data Processor e.g. an IT services provider? – [see Guidance Notes for the definition of Data Processor]. If yes, provide details of selection criteria, processing instructions and contract (may be attached separately).**

There are appropriate contracts, service level agreements and/or data processing agreements in place with Data Processors.

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

StormID Ltd – 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-ACDA-ADCD851430C4/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)	<p>NSS have a suite of policies including but not limited to:</p> <ul style="list-style-type: none"> • NSS Access Control Policy V1.2 • NSS Clear Desk Policy V1.1 • NSS Clear Screen Policy V1.1

Type of Control – examples	Description
	<ul style="list-style-type: none"> • 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 • National Notification System SSP • Destruction Process for hard drives and mobile phones – CST • NSS Data Cleansing Guidelines • Decommissioning and destruction of IT desktop devices <p>PHS has equivalent polices as listed above, in addition PHS has:</p> <ul style="list-style-type: none"> • Records Management, Document Storage, and Retention Policy V1.0 • Data Protection Policy V1.0 <p>Health Boards Each Health Board will have equivalent polices as listed above.</p> <p>Microsoft Azure NHS Scotland Azure Environment.</p> <p>Microsoft Azure has completed Level 2 of the NHS IG Toolkit. (https://download.microsoft.com/download/7/F/6/7F6EBDDDE-F3EF-4225-ACDAADCD851430C4/NHS_IG-Compliance.pdf)”</p> <p>Storm ID Lenus Storm ID is Cyber Essentials Plus certified. The solution adheres to the five technical controls of Cyber Essentials:</p> <ul style="list-style-type: none"> · 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 <p>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.</p>
Staff training	<p>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.</p> <p>PHS staff are required to complete mandatory Information Governance Training and have equivalent policies and procedures.</p> <p>NHS Scotland staff also receive mandatory IG training and Confidentiality also forms part of their employment contract.</p> <p>Microsoft Azure staff are trained to ensure they meet their own legal</p>

Type of Control – examples	Description
	<p>obligations.</p> <p>Storm ID staff are trained and vetted to ensure they meet their own legal obligations.</p>
<p>Adverse event reporting and management</p>	<p>NSS have an Adverse Events Management Policy and should be followed as appropriate. Staff can report any adverse events via qPulse, our adverse events portal.</p> <p>PHS have an adverse events policy which should be followed as appropriate.</p> <p>Health Boards will have their own adverse events policies and adverse events systems such as Datix.</p> <p>All contracts and agreements include data protection provisions and what data processors should do in the event of a data or security breach.</p>
<p>Physical access and authorisation controls</p>	<p>NSS have identify management systems, including role based access, in place. Further details can be found in the NSS Access Control Policy V1.2 - section 5 page 5.</p> <p>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:</p> <ul style="list-style-type: none"> • Working at home and working from home Policy • Remote Access Policy <p>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.</p> <p>PHS have equivalent polices as listed above and in addition, PHS has:</p> <ul style="list-style-type: none"> • Records Management, Document Storage, and Retention Policy V1.0 • Data Protection Policy V1.0 <p>Health Boards have equivalent or similar policies and procedures.</p> <p>Microsoft Azure have equivalent or similar policies to ensure they meet their own legal obligations.</p> <p>Storm ID train and conduct vetting on all of their staff. They have equivalent or similar policies to ensure they meet their own legal obligations.</p>
<p>Environmental controls</p>	<p>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 .</p> <p>The Routing Service sits in the NDP and so is also hosted in the Microsoft Azure Cloud.</p> <p>ECOSS - SSP being developed, however, penetration testing has been completed and the risks highlighted have been actioned.</p>

Type of Control – examples	Description
	<p>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.</p> <p>StormID Ltd – The data platform providing patient information storage and processing platform, 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. (https://download.microsoft.com/download/7/F/6/7F6EBDDE-F3EF-4225-ACDA-ADCD851430C4/NHS_IGCompliance.pdf)</p>
<p>Information asset management including management of backups and asset disposal</p>	<p>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.</p> <p>We also have the following procedures:</p> <ul style="list-style-type: none"> • Destruction Process for hard drives and mobile phones – CST • NSS Data Cleansing Guidelines • Decommissioning and destruction of IT desktop devices <p>PHS have equivalent policies as listed above and in addition, PHS has:</p> <ul style="list-style-type: none"> • Records Management, Document Storage, and Retention Policy V1.0 • Data Protection Policy V1.0 <p>Health Boards have equivalent or similar policies and procedures. Storm ID IT team are responsible for maintaining Information Backup controls.</p> <p>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 infrastructure and application code can be redeployed to a previously known and working state in minutes.</p> <p>DR scenarios and RPOs/RTOs are factored into solutions where necessary.</p>
<p>Business continuity</p>	<p>A disaster recovery plan was produced as part of the project to implement the CDW system and a backup Ensemble server is in place for business continuity.</p> <p>A SSP for ECOSS is being developed. NNS has a completed SSP. NDP Routing Service has a completed SSP.</p>

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

Type of Control – examples	Description
System access levels and user authentication controls	<p>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.</p> <p>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.</p> <p>Additional clinical users will be provisioned (and removed from the system when required) by the superuser.</p> <p>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.</p> <p>The NNS SSP covers this in detail. NSS also have an Access Control Policy V1.2.</p> <p>PHS have an equivalent or similar Access Control Policy.</p> <p>Health Boards have equivalent or similar policies and procedures.</p>
System auditing functionality and procedures	<p>NSS - NSS Information Security Policy V1.5 Section 6 – Responsibilities – page 6-7.</p> <p>All NSS staff follow the NSS Adverse Events Management policy and all our systems are auditable.</p> <p>There are audit logs that can be used to monitor access or for future investigations should a breach or incident be detected.</p> <p>PHS - Have equivalent or similar policies.</p> <p>Health Boards - Have equivalent or similar policies.</p> <p>Storm ID - The solution has database audit controls in place which audit database events and queries.</p>
Operating system controls such as vulnerability scanning and anti-virus software	<p>Storm ID application testing includes:</p> <ul style="list-style-type: none"> · Functional testing · Regression testing · Browser and device testing · Exploratory Testing · Performance testing · Security scanning testing

Type of Control – examples	Description
	<p>· Security Penetration testing</p> <p>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 lifecycle to actively seek out and fix vulnerabilities in the system such as out of date software versions.</p> <p>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.</p> <p>NDP - Security Penetration testing on each major release of platform. Automated scanning of the application as part of every deployment.</p> <p>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.</p> <p>Microsoft Azure: https://download.microsoft.com/download/7/F/6/7F6EBDDE-F3EF-4225-ACDAADC851430C4/NHS_IG-Compliance.pdf”</p> <p>NSS Information Security Policy V1.5 Section 5 - Information Security Policy Principles - page 5-6; Section 6 – NSS Responsibilities – page 6-7.</p>
Network security such as firewalls and penetration testing	<p>NSS has an extensive range of network security tools as detailed in the CDW SSP.</p> <p>The solution is cloud-based, so adheres to cloud security principles.</p>
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 and the web based application are cyber essentials plus certified.
System Security Policy (SSP) and Standard Operating Procedures(SOPs) (if applicable/ when available)	<p>There is an SSP for the Corporate Data Warehouse.</p> <p>There is an SSP for the NSS Ensemble.</p> <p>An SSP for ECOSS is being developed, however, penetration testing has been completed and the risks highlighted have been actioned.</p> <p>There is also a SSP for the NDP Routing Service.</p> <p>There is a SSP for National Notification System as well as NNS User Guide and NNS Demographics set up.</p>
Details of ISO27001/02 accreditation (if applicable)	<p>Accreditation for this standard is not necessary within NHSS however the Information Security Management System (ISMS) and SG policy that we work to in this area is consistent with the standard.</p> <p>Microsoft Azure has completed Level 2 of the NHS IG toolkit.</p>

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.

As this work was in response to the Covid 19 Pandemic. A rapid assessment was completed prior to this full impact assessment. The Data Protection Officers for NHS National Services Scotland, Public Health Scotland and the Scottish Government have been consulted. IG leads for all NHS Scotland Health Boards were also consulted.

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

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

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

16. Risks and actions identified [see Guidance Notes for more information].

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	<ul style="list-style-type: none"> • Due diligence in respect of national risk assessments/SSPs completed with appropriate sign-off. ECOSS is awaiting a SSP which is being developed, however, penetration testing has been completed and the risks have been 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 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.	3.23 3.24 3.25 3.26 3.27 3.28	Possible	Major	MODERATE	<ul style="list-style-type: none"> • 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.	3.23 3.24 3.25 3.26 3.27 3.28	Likely	Moderate	MODERATE	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. Risk of the text/email message going to the wrong person.	3.2	Possible	Moderate	MODERATE	<ul style="list-style-type: none"> Patients provide their details. Double input to highlight any errors. 	VERY LOW	Public Health Scotland; National Services Scotland; Medical Directors/SIROs , Territorial Boards	7 th July 2020
6. 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	<ul style="list-style-type: none"> 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 	VERY 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
					Government. <ul style="list-style-type: none"> Updated privacy notices from Scottish Government. Procedures in place to facilitate for rights compliance 			
7. Problems with the accuracy of data used in the process.	3.11	Possible	Moderate	MODERATE	<ul style="list-style-type: none"> Data as recorded by Special and Territorial Boards to be used for main records. Process to correct data available from all parties. Exceptions process is in place to assist with both data quality and CHI matching 	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	<ul style="list-style-type: none"> 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

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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. 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-	3.22 3.23 3.24	Possible	Major	MODERATE	<ul style="list-style-type: none"> 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 	LOW	National Services Scotland; Public Health Scotland	3 rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
residents may make unauthorised copies e.g. take screen shots on their phones etc of patient details, thereby causing a data breach.					home, who may be listening and the breaches this can lead to. <ul style="list-style-type: none"> 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. Homeworking policy will be in place. 			
12. Inappropriate access to information due to others living in a household.	3.22 3.23 3.24	Possible	Major	MODERATE	<ul style="list-style-type: none"> Staff will have a username and password that they should not share with others. They will have access to the minimum required data in order to complete their tasks. Staff will receive training in regards to data protection and confidentiality. It has been highlighted that it's a disciplinary 	LOW	National Services Scotland	3 rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					offence and also a criminal matter as per section 170 of the Data Protection Act 2018. <ul style="list-style-type: none"> All user actions are recorded as part of the service of the application audit logs. Homeworking Policy will be in place 			
13. Availability Breach	3.23 3.24 3.25 3.26 3.27 3.28	Possible	Major	MODERATE	<ul style="list-style-type: none"> 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 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 	LOW	National Services Scotland	3 rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					server.			
14. Systems can be at risk from human error at system supplier level (e.g. programming error)	3.11 3.20	Unlikely	Major	MODERATE	<ul style="list-style-type: none"> Appropriate testing by supplier and users 	LOW	National Services Scotland; Processors	3 rd July 20
15. There is a risk that the personal data is used for other purposes than for what it was originally intended for	3.1 3.4 3.5 3.6 3.7 3.20 3.25	Unlikely	Major	MODERATE	<ul style="list-style-type: none"> Data will only be used for the purposes outlined in this DPIA. Any further purposes identified would only be considered if they were compatible with the original purpose. Any further purposes would be subject to a rapid assessment and DPIA. 	LOW	National Services Scotland; Public Health Scotland	3 rd July 20
16. There is a risk that personal data is retained for longer than necessary.	3.17	Possible	Major	MODERATE	<ul style="list-style-type: none"> 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 	LOW	National Services Scotland; Public Health Scotland; SIRO's	3 rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					<p>they look to collect initially.</p> <ul style="list-style-type: none"> 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. There will be a research value for Covid 19 data, all such requests will be subject to further approvals and independent oversight. 			
17. There is a risk that the personal data is no longer relevant.	3.17	Possible	Major	MODERATE	<ul style="list-style-type: none"> 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	3 rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
18. There is a risk that personal data is passed to external organisations.	3.18 3.19	Unlikely	Major	MODERATE	<ul style="list-style-type: none"> No data will be shared with organisation's other than those listed within this DPIA. 	VERY LOW	National Services Scotland; Public Health Scotland	3 rd July 20
19. There is a risk that excessive personal data is collected on an individual.	3.1 3.2 3.7	Unlikely	Minor	LOW	<ul style="list-style-type: none"> Datasets have been developed to only collect the information necessary. Datasets provided within the DPIA. 	VERY LOW	National Services Scotland; Public Health Scotland	3 rd July 20
20. 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	<ul style="list-style-type: none"> 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. 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	3 rd July 20
21. Relevant or new data processors may not all have adequate data processing	3.20	Unlikely	Moderate	LOW	<ul style="list-style-type: none"> Contracts and Data Processing Agreements are in place with known relevant processors. 	VERY LOW	National Services Scotland; Public	3 rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
agreements in place					<ul style="list-style-type: none"> 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 		Health Scotland; SIRO's	
22. 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 3.32 3.33 3.34 3.35 3.36 3.37 3.38	Possible	Major	MODERATE	<ul style="list-style-type: none"> 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	3 rd July 20

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
23. Personal data for additional phases of this process, may not be encrypted both/either in transit or at rest	3.35	Unlikely	Major	MODERATE	<ul style="list-style-type: none"> 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	3 rd July 20
24. 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	<ul style="list-style-type: none"> Review policies regularly 	LOW	National Services Scotland; Public Health Scotland;	8 th July 2020
25. There is a risk that someone in the same household could access the results of someone they live with via access to their phone etc.	3.1	Possible	Moderate	MODERATE	<ul style="list-style-type: none"> Patients provide their data. Link sent to their results via email or text message. Verification required. Patients are responsible for 	LOW	National Services Scotland; Public Health Scotland; Patients	22 nd July 2020

Description	DPIA Section	Likelihood	Consequence	Overall Risk rating	Mitigation/ Actions	Residual Risk	Risk Owner	Date
					managing their own devices and ensuring these are secure by using passcodes/passwords.			

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: Every 6 months

GUIDANCE NOTES

Question 2 - Special category personal data

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

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

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

Question 3 – Legal condition

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

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

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

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

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

- 9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law
- 9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement

- 9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- 9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- 9(2)(e) – Processing relates to personal data manifestly made public by the data subject
- 9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- 9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional
- 9(2)(i) – Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- 9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

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

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

Question 10 – Data Processor

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

Question 16 – Risk Assessment

ASSESSING THE RISK LEVEL

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

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

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

When determining the likelihood you should consider:

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

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

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

Examples of **Events**:

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

Examples of **Impacts**:

- Only 1 data subject affected but significant or extreme consequences e.g. missed vital treatment as a consequence of information not being issued to the patient or health professional leading to death or major permanent incapacity.
- Very sensitive data being exposed to people who don't need to know causes extreme distress (could be patient or staff data).
- Large amount of non-sensitive but personal identifiable data lost in the wind when in transit causing organisational embarrassment in the news for a week.
- Staff snooping neighbours medical records.
- Excessive health data shared with social worker (husband under domestic abuse investigation) causing direct threats and stalking.

- Personal health data shared by a charity with private business for commercial/marketing purposes causing unwanted disturbance.
- Reportable data breach to ICO causing monetary penalty.
- Complaint from patient to ICO results in undertaking for better access to health records.
- 1.6 million patients in Google Deepmind.
- Compliance Audit recommended.
- DC action required.
- Undertaking served.
- Advisory Visit recommended.
- Improvement Action Plan agreed.
- Enforcement Notice pursued.
- Criminal Investigation pursued.
- Civil Monetary Penalty pursued.

Which impact do you opt for?

NOT worst case scenario

NOT most likely scenario

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

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

3. Determine the **RISK** rating $L \times I = R$ using the IRMA approach