

Data Protection Impact Assessment (DPIA) – template for report

This template was developed by the SG Data Protection and Information Assets team.

This template was last updated in June 2018.

Before conducting the [Data Protection Impact Assessment](#), please refer to the guidance that accompanies this template.

1. Introduction

Public Health Scotland will be a new public body created in Scotland under section 2 of the National Health Service (Scotland) Act 1978 (the 1978 Act). It will be constituted as a national Special Health Board, taking over the current functions and data responsibilities of Health Protection Scotland, Information Services Division and NHS Health Scotland. This Data Protection Impact Assessment (DPIA) looks at the implications of the transfer of those data functions.

It should be noted that this DPIA will be reviewed again in the coming months before the establishment of Public Health Scotland. This will ensure that an up-to-date assessment of impact has been carried out in conjunction with key stakeholders.

2. Document metadata

2.1 Name of Project: **Establishing Public Health Scotland**

2.2 Author of report: **Robert Girvan and Asif Ishaq**

2.3 Date of report: **17 October 2019**

2.4 Name of Information Asset Owner (IAO) of relevant business unit: **Derek Grieve**

2.5 Date for review of DPIA:

Review date	Details of update	Completion date	Approval Date
Early January 2020	Exact details to be confirmed but we will seek to determine what information assets will move to Public Health Scotland.	End January 2020	
Early March 2020	Any further updates reflected in a revised DPIA before vesting date.	End March 2020	

3. Description of the project

3.1 Description of the work:

The new public health model seeks to deliver better health and wellbeing outcomes for communities by promoting a collaborative approach to planning and delivery, putting decision making in the hands of local communities and agencies who are best-placed to assess local public health needs. At

national level a new Special Health Board, called Public Health Scotland, will provide strategic leadership; enhanced opportunities for innovation, research, learning and development; and assurance on the delivery of improved population health outcomes.

Under the new model, the bodies of: Health Protection Scotland (a division of NHS National Services Scotland (NSS) and part of Public Health and Intelligence (PHI)); Information Services Division (also a division of NSS and part of PHI); and NHS Health Scotland (a Special Health Board) will cease to exist and Public Health Scotland will take over all of their current functions and services. This includes the transfer of significant data responsibilities related to health information, health intelligence, statistical services and advice that supports the NHS in progressing quality improvement in health and social care and facilitates robust planning and decision making. Public Health Scotland will be responsible for delivering all the Information Governance and statistical governance responsibilities of the predecessor bodies. It will also need to replicate the data sharing agreements that are in place for these bodies and ensure that any relevant data still collected and stored centrally by NSS, or other parties, can continue to be accessed and processed safely and effectively.

Public Health Scotland will have to comply with all relevant legislation and put in place policies, procedures and data sharing agreements - as per the predecessor bodies - ensuring that any relevant data collected and stored complies with the required legislation, and any data collected and stored by other parties can continue to be accessed and processed securely and effectively. This includes meeting requirements for Data Protection Impact Assessments, relevant training and data processor arrangements.

Under data protection laws, the new public health body will have responsibilities to respond to subject access requests when a member of the public wants to see information that they hold about them. It will also respond to public requests for information under the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information Regulations 2004 (EIR). Under The Official Statistics (Scotland) Order 2008 NSS currently have statutory powers to produce official statistics for NHS Scotland. Responsibility for production of health statistics will transfer to Public Health Scotland from NSS. The statistical governance team in Public Health Scotland will need to ensure that official statistics are produced in accordance with the Code of Practice for Statistics 2018 which ensures that statistics are trustworthy, of high quality and of public value.

The new organisation will have a designated Data Protection Officer (DPO) and a Senior Information Risk Owner (SIRO) and will put in place appropriate technical and organisational measures in order to meet the accountability data protection principle. Public Health Scotland will need to build in privacy by default and design and it will require the ability to remove an individual's data from the dataset, or a robust reasoned opinion as to why that may not be possible. The new body will adopt and publish statements on its Statement of Public Task – which will need to be prepared in advance of vesting day. <https://nhsnss.org/media/2595/statement-of-public-task.pdf>

Public Health Scotland will be a knowledge based and intelligence driven organisation with a critical reliance on data and information to enable it to fulfil its statutory duties and accomplish its vision of achieving better health and wellbeing outcomes for the population. As such, it will need access to a wide range of data and information from across the whole system. The ability to effectively and efficiently identify and respond to immediate threats and longer term challenges to public health depends on it having timely and efficient access to data and information on the health and wellbeing status of the population, the wider determinants of health across populations, and the provision of health and care services to the population of Scotland.



Our intention is that the accessibility of the data to those who need it will be maintained and ultimately enhanced. This includes the timeliness of access as well as consideration of the fundamental confidentiality and security requirements related to the data access. Our ambition is that all parts of the system should work together to gain maximum value from data, including optimising functionality and linkages across the system, securing Best Value for the public, and translating the data into intelligence that can help improve health and wellbeing outcomes. In the short-term we want to be assured that the new body has the capacity and capability to achieve the data function transfer without any degradation of quality and performance or any impact on other core functions. The ultimate, long-term aim is to enable the effective and efficient sharing of data wherever and whenever it is required for direct clinical care, population health management, and intelligence and research.

In carrying out this transfer of data and intelligence functions, we recognise that ensuring privacy, security and good governance are paramount. Public Health Scotland will build good relationships with the NHS, Government, local authorities, research bodies and other data controllers. This will be instrumental to facilitate access to data, ensure proportionate governance and improve data linkage.

As with its predecessor bodies, Public Health Scotland will use personal information on different groups of people including:

- patients;
- staff and volunteers;
- contractors;
- suppliers;
- complainants, enquirers;
- people who've responded to surveys;
- professional experts and consultants.

For example, Public Health Scotland will use personal information to:

- support the administration of its services;
- report on activities of health and care services, including national audits and official statistics;
- monitor health hazards for the people of Scotland by gathering surveillance information provided by laboratories, hospitals, GPs, NHS Boards and Local Authorities;
- manage exposure to health hazards and large outbreaks of infectious illness that may affect many people across Scotland, such as large flu outbreaks;
- link data from different sources where that is required to deliver its functions;
- conduct research and provide support and data for external researchers;
- support and manage employees;
- maintain accounts and records.

Any personal information used will include 'special category data' defined specifically in the General Data Protection Regulation (GDPR) as:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;



- sex life or sexual orientation.

In the majority of cases, people will not provide information directly to Public Health Scotland, it will be received from other individuals and organisations involved in the delivery or support of health and care services in Scotland.

These include:

- other NHS boards;
- primary care contractors such as GPs, dentists, pharmacists and opticians;
- other public bodies, for example local authorities;
- research bodies and universities;
- suppliers of goods and services.

Public Health Scotland will process information for the purpose of fulfilling its statutory functions and its services. The body may also disclose the information to a third party where it has a legal basis to do so.

Under the Public Health (Scotland) Act 2008, NHS staff will be required to notify Public Health Scotland and provide personal information about the person affected when someone contracts a specific (notifiable) disease, or a laboratory identifies a notifiable organism, or a professional identifies a 'health risk state' as defined under the Act.

Public Health Scotland will have responsibilities as a 'data controller'. A data controller decides why and how personal information is used. This means that they need to have a legal basis when using personal information.

The tasks and functions Public Health Scotland will perform are in the public interest. This means that the legal basis for their using personal information will usually be that the information is needed for performing a task they are carrying out in the public interest, or exercising official authority vested in them.

In some situations Public Health Scotland may rely on a different legal basis – for example, the legal basis for using personal information to pay a supplier is that the information is needed for the purposes of their legitimate interests as a buyer of goods and services.

The legal basis when Public Health Scotland will use more sensitive types of personal information, including health information, will usually be that the use is necessary:

- for providing health or social care or treatment or managing health or social care systems and services;
- for reasons of public interest in the area of public health;
- for purposes of preventive or occupational medicine, the provision of health or social care or the management of health or social care systems and services;
- for archiving, scientific or historical research purposes or statistical purposes;
- in order to protect the vital interests of an individual;
- for establishing, exercising or defending legal claims or in the case of a court order.

On rare occasions Public Health Scotland may rely on explicit consent as the legal basis for using personal information. When they do this they will explain what it means, and the rights that are available to the individual.



Proportionality is a key principle Public Health Scotland will adhere to in all information sharing. Anonymisation or pseudonymisation will be carried out wherever possible to preserve the privacy and confidentiality of the individual.

3.2 Personal data to be processed.

Variable	Data Source
To be confirmed following discussion with key stakeholders regarding the specific information assets to be transferred to Public Health Scotland.	

3.3 Describe how this data will be processed:

As with its predecessor bodies, Public Health Scotland will use personal information on different groups of people including:

- patients
- staff and volunteers
- contractors
- suppliers
- complainants, enquirers
- people who've responded to surveys
- professional experts and consultants
- individuals captured by CCTV.

Along with all health boards within NHS Scotland, Public Health Scotland will use personal information to:

- support the administration of health and care services
- construct datasets in relation to health and care services and the determinants of health and wellbeing
- carry out data matching under the national fraud initiative, in conjunction with NSS practitioner services
- conduct and support research
- support and manage employees
- maintain accounts and records
- use CCTV systems for crime prevention

They will use personal information to help deliver the following existing services:

Co-ordinating and supporting specialist national services to help protect Scotland's people from infectious and environmental hazards – [visit our Health Protection Scotland \(HPS\) website](#) (external link).

Supporting better decision-making using health information and statistics – [visit our Information Services Division website](#) (external link).



Working to reduce health inequalities and improve population health in Scotland - <http://www.healthscotland.scot/>

The Scottish Public Health Observatory ([ScotPHO](#)) also brings together a wide variety of high quality data, profiles and reports on the health of Scotland's population. ScotPHO is a collaboration led by NHS Health Scotland and ISD Scotland. The wealth of public health information available on the ScotPHO website includes their online profiles tool which allows you to access a wide variety of data for your local area and for Scotland.

The personal information used will include information that identifies individuals like their name, address, date of birth and postcode.

The information used can relate to:

- personal and family details
- education, training and employment
- financial details
- lifestyle and social circumstances
- goods and services
- visual images
- details held in patient records
- responses to surveys.

Sensitive personal information

Public Health Scotland will also use more sensitive types of personal information, including information about:

- racial or ethnic origin
- religious or philosophical beliefs
- trade union membership
- health
- sex life or sexual orientation
- criminal convictions and offences.

Who provides the personal information

In the main, information will not be directly provided individuals but, rather, organisations that are involved in the delivery of health and care services in Scotland. These include:

- other NHS boards
- primary care contractors such as GPs, dentists, pharmacists and opticians
- other public bodies, for example local authorities
- research bodies and universities
- suppliers of goods and services.

Processing

Public Health Scotland will process information for the purpose of fulfilling its statutory functions and providing people with its services. The main functions are around analysis, planning, research and standards. Information will include some or all of the following:



- Managing enquires, requests and complaints.
- Providing opportunities to give feedback on their products and services, to help gauge need and improve products and services appropriately.
- Providing people with e-newsletters they have opted in to receive.
- Allowing people to subscribe and comment on blogs.
- Conducting data and statistical analysis to monitor performance of services and make improvements.
- Assessing how safe and effective a treatment is.
- Checking that the NHS is providing a good service and spending public money properly.
- Planning how many beds, clinics and staff are needed.
- Monitoring particular illnesses or diseases (epidemiology).
- Carrying out public health or clinical research.
- Reporting on performance against national treatment standards and targets required by the Scottish Government.
- Reporting on current and future costs and numbers of NHSScotland staff.

Public Health Scotland may share complaints information with the relevant NHS board or Scottish Government department if the complaint or concern has been sent to them in error, or where a joint response is required.

They may also disclose the information to a third party where they have a legal basis to do so.

3.4 Explain the legal basis for the sharing with internal or external partners:

As an organisation, Public Health Scotland will be delegated functions by the Scottish Government as a Special Health Board so they can promote and improve the physical and mental health of the people of Scotland and play their part in operating a comprehensive and integrated national health service in Scotland.

These tasks (or functions as they are described in the legislation), will be delegated to them under the National Health Service (Scotland) Act 1978 by Order.

Under data protection laws, and other relevant legislation, Public Health Scotland will have responsibilities as a 'data controller'. A data controller decides why and how we use personal information. This means that they need to have a legal basis when using personal information.

We consider that the tasks and functions Public Health Scotland will perform are in the public interest. This means that the legal basis for using personal information is usually that the information is needed for performing a task they are carrying out in the public interest, or exercising official authority vested in them.

In some situations Public Health Scotland may rely on a different legal basis – for example, the legal basis for using personal information to pay a supplier is that the information is needed for the purposes of their legitimate interests as a buyer of goods and services.

The legal basis when Public Health Scotland will use more sensitive types of personal information, including health information, is usually that the use is necessary:

- for providing health or social care or treatment or managing health or social care systems and services;



- for reasons of public interest in the area of public health;
- for reasons of substantial public interest for aims that are proportionate and respect people’s rights, like research;
- in order to protect the vital interests of an individual; and
- for establishing, exercising or defending legal claims or in the case of a court order.

On rare occasions Public Health Scotland may rely on explicit consent as the legal basis for using personal information. When it does this it will comply with the requirements and responsibilities under DP laws for relying on individual consent.

The Scottish Government’s Public Bodies (Joint Working) (Scotland) Act 2014 (2014 Act) also requires each Health and Social Care Integration Authority to produce joint commissioning strategies and delivery plans. The Common Services Agency for the Scottish Health Service (commonly known as NSS) has been commissioned to work in partnership with the Scottish Government, NHS Health Boards, Local Authorities, Health and Social Care Integration Authorities and other stakeholders in a collaborative manner to develop and improve the information available to Integration Authorities on an ongoing basis in order to support their needs. Public Health Scotland will take over this responsibility.

The aim of the Collaboration generally is to provide Health and Social Care Integration Authorities with nationally linked multiple data sources across multiple sectors and public services to provide a broader range of Service User and individual level data. This information will support Integration Authorities to assess and forecast needs, link investment to agreed desired outcomes, consider options, plan and evaluate the nature, range and quality of services, provide transparent and comparable evidence to progress in achieving Health and Social Care outcomes.

As part of the Project social care activity data, at a Service User level, will be submitted to Public Health Scotland via an agreed secure transfer mechanism for linkage to NHS health records.

INFORMATION SHARING

Generally speaking, information sharing is a complex issue within the NHS. There are very few examples of *specific* information sharing powers. The undernoted main (but not exclusive) issues all need to be considered.

- Data Protection legislation
- Human Rights legislation
- Common law duty of confidentiality.
- Public Health (Scotland) Act
- Ethical guidance
- Professional guidance

Information sharing powers

Specific information sharing powers for NSS and NHS HS are limited. In the context of health and social care integration, Section 49 of the Public Bodies (Joint Working) (Scotland) Act 2014 (“**2014 Act**”) provides that the Local Authority, Health Board and Integration Joint Board can share information amongst them in relation to planning and carrying out of integration functions. This is regardless of any duty of confidentiality owed to any person in relation to the information disclosed. In other words, it sets aside the common law duty of confidentiality.



HPS, ISD (NSS) and Health Scotland are not named in the list of bodies that can use Section 49 and similarly we do not envisage that Public Health Scotland will be named.

There are no other obvious examples of specific powers to share *generally*. There are various situations when certain information *must* be shared (e.g. Section 15 of the Public Health (Scotland) Act 2008 in relation to notification of communicable diseases).

Data Protection Legislation

In terms of the use by Public Health Scotland of information *from another NHSS organisation or other public body*, PHS requires to satisfy conditions for processing. Article 6(1)(e) GDPR (necessary for the performance of a public task) is generally used for the Article 6 condition. The public task could for example be the collection and dissemination of epidemiological data as to be set out in the Public Health Scotland Functions Order. With a focus on the current activities of ISD, Article 9(2)(j) GDPR (necessary for archiving, scientific or historical research purposes or statistical purposes) is often used for the Article 9 condition. The following Article 9 conditions may also be relevant for PHS:

- Articles 9(2)(f) (necessary for legal claims), 9(2)(g) (necessary for reasons of substantial public interest), 9(2)(h) (necessary for health and social care purposes (which includes the management of health and social care systems)) and 9(2)(i) (necessary for reasons of public interest in the area of public health) may also be applicable.

Human Rights

In order for the sharing of personal information to comply with Article 8 of the ECHR, any interferences with the right must be in accordance with law, be in pursuit of legitimate aims (which are set out in Article 8(2) and include protection of health) and be necessary in a democratic society (i.e. there needs to be a pressing social need). Proportionality is a key principle we will adhere to here and provided the other main issues mentioned above are satisfied, satisfying Article 8 should not be a problem.

Common Law Duty of Confidentiality

Where the common law duty of confidentiality is not set aside by statute then NHSS generally requires to look at the exemptions available. These are consent (which is set at a much lower bar than that required under Data Protection legislation) where disclosure is necessary to safeguard the individual or others, or is in the public interest, or where there is statutory basis or a legal duty to disclose.

In the context of information sharing within NHSS for the treatment of individuals, the consent (albeit implied) of the individual is generally relied on. For other matters (including research), the public interest exemption is generally used.

Other Legislation

Other legislation will also have to be complied with such as:

- The Public Health (Scotland) Act 2008



- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers (Scotland) Act 2000
- Freedom of Information (Scotland) Act 2002
- The Official Statistics (Scotland) Order 2008
- The Official Statistics (Scotland) Amendment Order 2012
- Statistics Code of Practice
- The Network and Information Systems Regulations 2018
- The Environmental Information Regulations 2004

4. Stakeholder analysis and consultation

4.1 List all the groups involved in the project, and state their interest.

Group	Interest
Scottish Government and Local Government (COSLA) leads	Shared leadership of Public Health Scotland.
NSS and NHS Health Scotland	Predecessor bodies.
Integration Authorities	Data collection and analysis to inform service delivery.
Community Planning Partnerships	Data collection and analysis to inform service delivery.
Research bodies and universities	Electronic Data Research and Innovation Service (eDRIS) and actual provision of data.
Third sector	Local intelligence support

4.2 Method used to consult with these groups when making the DPIA.

Consultation has been undertaken via the Public Health Oversight Board, Public Health Reform Programme Board.

A formal public consultation on the proposals for the new public health body was launched in May 2019: “A consultation on the new National Public Health Body ‘Public Health Scotland’” seeking views on the role, structure and expected functions of Public Health Scotland, with some discussion of its interface with other bodies, partnerships and statutory frameworks. It also sought views on questions related to proposals for the new public health body on information governance, data and intelligence function, data science and innovation. The consultation closed on 8 July 2019 and a total of 185 responses were received. The analysis of responses report was published on 14 August 2019. The report can be accessed here: <https://www.gov.scot/publications/public-health-scotland-analysis-responses-public-consultation/>.

Lastly, there has been considerable engagement and analysis across sectors in the context of the reform programme, including public engagement events, oversight boards and a series of collaborative commissions, including one specifically on data and intelligence, which describe the functions of the new body. Further details are available on the Public Health Reform website: <https://publichealthreform.scot/>.

4.3 Method used to communicate the outcomes of the DPIA



Via the Public Health Oversight Board, Public Health Reform Programme Board and analysis of responses report on the public consultation, which was published on 14 August 2019. The report can be accessed here: <https://www.gov.scot/publications/public-health-scotland-analysis-responses-public-consultation/>. The DPIA will also be published on both the Scottish Government and Public Health Reform websites.

5. Questions to identify privacy issues

5.1 Involvement of multiple organisations

Yes - NHSS, local government, third sector, health and social care integration authorities, and research bodies/universities.

5.2 Anonymity and pseudonymity

Anonymisation and pseudonymisation will be carried out wherever possible to preserve and respect the privacy and confidentiality of the individual.

5.3 Technology

To be determined following discussion with key stakeholders.

5.4 Identification methods

Existing unique identifiers such as CHI numbers will be used.

5.5 Sensitive/Special Category personal data

Yes, various sensitive types of personal information will be involved as outlined above.

5.6 Changes to data handling procedures

It is likely that there will be no substantive changes to data handling procedures although this will depend on the specific information assets to be transferred to the new body.

5.7 Statutory exemptions/protection

No specific exemptions.



5.8 Justification

The project is a key part of the Public Health Reform programme that emanated from the Christie Commission report (2011) recommendations and the Public Health Review (2015) and Health & Social Care Delivery Plan (2016).

5.9 Other risks

None identified in addition to the issues covered in the questions above.

6. General Data Protection Regulation (GDPR) Principles

Principle	Compliant Yes/No	Description of how you have complied
6.1 Principle 1 – fair and lawful, and meeting the conditions for processing	Yes	Public Health Scotland (PHS) will obviously take its responsibilities, under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), seriously and, as a Special Health Board, will adopt a Data Protection Policy, which sets out its commitment to compliance. To this end, it will appoint a 'Caldicott Guardian' (as well as a Data Protection Officer (DPO) and Senior Information Risk Owner (SIRO)) whose role will be to advise the Board and oversee how the new organisation uses patient identifiable information and enforces patients' rights to confidentiality. All PHS staff will be contractually obliged to respect confidentiality and provided with a set of Confidentiality Rules which govern how personal data is handled, stored, transmitted and disposed of.
Principle	Compliant Yes/No	Description of how you have complied
6.2 Principle 2 – purpose limitation	Yes	PHS will collect information about service users and organisations when they access any of their services online, by phone, in person, or in writing. They will only collect the information they ask for, that is given to them and, where required, has consent to it being processed for the purpose of providing NHS Health Scotland's services.
Principle	Compliant Yes/No	Description of how you have complied
6.3 Principle 3 – adequacy, relevance and data minimisation	Yes	PHS will process individual-related information in order to provide the population with required services, to monitor and improve health, improve health and care quality and safety and manage public health risks to health of the population. This includes some or all of the following: <ul style="list-style-type: none"> •Conducting data and statistical analysis to monitor performance of their services and make improvements. •Managing enquires, requests and complaints. •Providing opportunities to give feedback on their products and services, to help them know what the public need and improve products and services appropriately. •Providing e-newsletters you have opted in to receive. •Allowing individuals to subscribe and comment on blogs.



		<p>PHS may share complaints information with the relevant NHS board or Scottish Government department if the complaint or concern has been sent to them in error, or a joint response is required.</p> <p>They may also disclose the information to a third party where they have a legal basis to do so. PHS will not share or sell personal information to any other organisation.</p>
Principle	Compliant Yes/No	Description of how you have complied
6.4 Principle 4 – accurate, kept up to date, deletion	Yes	<p>To meet these requirements PHS will:</p> <ul style="list-style-type: none"> • update individual data or remove it from their systems at the individual's request. It may challenge a request for deletion on the grounds that the public interest condition requires us to keep full population information. In accordance with Data Protection laws, PHS would, of course, give individual consideration to all legitimate requests to exercise subject rights. • include details of how to unsubscribe within any e-newsletters individuals have signed up to receive • keep data in line with NHSScotland data retention guidelines.
Principle	Compliant Yes/No	Description of how you have complied
6.5 Principle 5 – kept for no longer than necessary, anonymization	Yes.	<p>PHS will keep personal information as set out in the Scottish Government Records Management: NHS Code of Practice (Scotland) Version 2.1 January 2012. The NHS Code of Practice sets out minimum retention periods for information, including personal information, held in different types of records including personal health records and administrative records. Personal information will be stored securely and only accessible to authorised people.</p> <p>Most PHS analysis will be undertaken with information that does not directly identify the individual. When another organisation requests information, it will only be released after removing as much information that could identify the individual as possible. PHS will only release information that could identify the individual directly when required or permitted by law, or when it can be shown that the individual concerned gave his/her permission.</p>
Principle	Compliant Yes/No	Description of how you have complied
6.6 GDPR Articles 12-22 – data subject rights	Yes	<p>Subject to the data protection conditions for processing, PHS will ensure you have the following rights:</p> <ul style="list-style-type: none"> •The right to be informed •The right of access •The right to rectification •The right to erasure •The right to restrict processing •The right to data portability •The right to object •Rights in relation to automated decision making and profiling.



		You may request a copy of the information that PHS hold about you, correct any information that is inaccurate, unsubscribe from their services, or withdraw your consent, by contacting the Data Protection Officer.
Principle	Compliant Yes/No –	Description of how you have complied
6.7 Principle 6 - security	Yes.	<p>The information PHS collect about you and your organisation will be stored securely in NHS Scotland systems hosted in the UK/EU.</p> <p>If you subscribe to an e-newsletter, your contact details will be stored in a list hosted on a secure server by a third party in the UK/EU.</p> <p>The website will be hosted on a secure server by a third party in the UK/EU, and maintained by Public Health Scotland staff.</p> <p>There are a number of policies and procedures that will help PHS to ensure that personal data is kept secure.</p> <ul style="list-style-type: none"> •Most of the analysis that they will carry out uses pseudonymised/anonymised information. This means that information that could directly identify an individual, for example name, date of birth or address is removed. •Only a limited number of specially trained staff can access confidential information that could identify a person. Access can only be given with individual role-specific permission that has to be renewed regularly •Statistical Disclosure Control is a way to reduce the risk of disclosing personally identifiable information. PHS will apply its statistical disclosure control guidelines to published information. •The Public Benefit and Privacy Panel for Health and Social Care decides when nationally held information about people who use health and care services can be used for research, audit and service improvement whilst upholding legal obligations of data protection and confidentiality. The panel is made up of doctors, lay members, researchers and specialist advisers on confidentiality and data protection. It considers if requests for information strike the right balance between protecting personal data and making data available for research and audit that has public benefit. It makes sure that any information releases are carefully controlled and in the public interest. •Any researcher wishing to use the data that PHS hold must follow current legal and ethical guidelines and comply with the specific instructions set out in the permissions given.
Principle	Compliant Yes/No –	Description of how you have complied
6.8 GDPR Article 24 - Personal data shall not be transferred to a country or territory outside the European Economic Area.	Yes.	Personal data will not be transferred to a country or territory outside the European Economic Area.



7. Risks identified and appropriate solutions or mitigation actions proposed

Is the risk eliminated, reduced or accepted?

Risk	Ref	Solution or mitigation	Result
Personal data is inadvertently shared outwith Public Health Scotland.		Detailed discussions planned with IT security and data intelligence project leads to discuss and agree transition of data sharing requirements, arrangements and protocols.	Reduce.

8. Incorporating Privacy Risks into planning

Explain how the risks and solutions or mitigation actions will be incorporated into the project/business plan, and how they will be monitored. There must be a named official responsible for addressing and monitoring each risk.

Risk	Ref	How risk will be incorporated into planning	Owner
Personal data is inadvertently shared outwith Public Health Scotland.		Data sharing requirements and protocols to be discussed and agreed prior to transfer of functions and staff to Public Health Scotland, including reference to legal advice if/where required.	Tbc. Possibly the SIRO or Caldicott Guardian.



9. Data Protection Officer (DPO)

9.1 The DPO may give additional advice, please indicate how this has been actioned.

Advice from DPO	Action
Not applicable as the new body does not yet exist. Once established, Public Health Scotland will appoint its own DPO.	

10. Authorisation and publication

The DPIA report should be signed by your Information Asset Owner (IAO). The IAO will be the Deputy Director or Head of Division.

Before signing the DPIA report, an IAO should ensure that she/he is satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken.

By signing the DPIA report, the IAO is confirming that the impact of applying the policy has been sufficiently assessed against the individuals' right to privacy.

The results of the impact assessment must be published in the eRDM with the phrase "DPIA report" and the name of the project or initiative in the title.

Details of any relevant information asset must be added to the Information Asset Register, with a note that a DPIA has been conducted.

I confirm that the impact of establishing the new public health body, Public Health Scotland, has been sufficiently assessed against the needs of the privacy duty:

Name and job title of a IAO or equivalent	Date each version authorised
Derek Grieve, Interim Head of Health Protection Division	21 October 2019

