Cefnogir gan
Lywodraeth Cymru
Supported by
Welsh Government

Wales Accord on the Sharing of Personal Information

COVID-19 Joint Controller Agreement

(for personal data necessary to deal with the COVID-19 outbreak only)

Implementing the Test, Trace, Protect strategy

Version 3.0

Review Date 03/10/2020

Issue date 24/07/2020

Internally assured on 23/07/2020

GUIDANCE NOTE

SEEK ADVICE FROM YOUR DATA PROTECTION OFFICER OR YOUR INFORMATION GOVERNANCE/MANAGEMENT LEAD BEFORE ENTERING INTO ANY JOINT CONTROLLER ARRANGEMENTS OR DRAFTING AN AGREEMENT. THEY WILL ADVISE ON THE APPROACH YOUR ORGANISATION IS TAKING TO RISK ASSESSING AND DOCUMENTING INFORMATION SHARING PRACTICES FOR COVID-19 PROJECTS OR INITIATIVES.

Dealing with the COVID-19 outbreak presents many challenges to public service providers. The Information Commissioner[1] and NHS Wales[2] have issued statements acknowledging both the need to work differently and the pace at which organisations need to make decisions. Both statements suggest a proportionate approach to data protection and information governance, including information sharing agreements. Welsh Government has also issued a letter encouraging organisations to consider the provisions available under regulation 3(1) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) to process confidential patient information.[3]

WASPI **Data Disclosure Agreements (DDAs**) are available to support one-way disclosures of personal data from one controller to another and could be of use to support COVID-19 work.

WASPI **Information Sharing Protocols (ISPs)** are designed to underpin two-way sharing of personal data between multiple controllers for a specific purpose. ISPs are more suited for projects that have established information exchanges. They are also subject to quality assurance processes, which may not provide the timely response required to support new and urgent arrangements aimed at dealing with the COVID-19 outbreak.

WASPI **Joint Controller Arrangement Check** provides some considerations to take into account when developing a Joint Controller arrangement.

*ISPs remain relevant to non-COVID-19 projects, programmes or innitiatives and should pass through the normal QA process. Contact your Data Protection Officer/Information Goverance lead or the WASPI Team for advice on how to proceed at this time.

[1] https://ico.org.uk/for-organisations/data-protection-and-coronavirus/

[2] https://nwis.nhs.wales/coronavirus/digital-support-updates-for-healthcare-professionals/information-governance/

[3] https://nwis.nhs.wales/coronavirus/coronavirus-content/coronavirus-documents/wg-letter-request-for-processing-confidential-patient-information-related-to-covid-19/

Document History

1. Author details		
Name:	Organisation:	Phone number / email:
John Sweeney	NHS Wales Informatics Service (NWIS)	John.Sweeney@wales.nhs.uk
Alun Kime	Flintshire County Council	Alun.Kime@flintshire.gov.uk
2. Who provided data protection advice?		
Name	*Organisation*	*Phone number / email:*
John Lawson	Public Health Wales	John.Lawson@wales.nhs.uk
Darren Lloyd	NWIS	Darren.Lloyd@wales.nhs.uk

Contents

1 About this agreement

1.1 This COVID-19 Joint Controller Agreement has been written in accordance with the principles contained within the Wales Accord on the Sharing of Personal Information (WASPI).

1.2 This is an overarching agreement between various parties who need to share personal data in order to deliver a coherent and collaborative response to the COVID-19 outbreak in Wales. The agreement focuses on the implementation of Welsh Government's Test, Trace, Protect strategy.

1.3 The schedules to this agreement provide further detail on the key information exchanges involved in the different elements of the strategy.

1.4 This Joint Controller Agreement is required under Article 26 of GDPR. Joint controllers are required in a transparent manner to agree their respective responsibilities for compliance. This agreement also demonstrates compliance and defines accountability which is an overriding principle of GDPR.

1.5 Partners include Public Health Wales, Local Health Boards and NHS Wales Trusts, Welsh Local Authorities and other stakeholders, such as NHS Wales Informatics Service and others who may be specifically referenced in the attached schedules.

1.6 The Data Protection Impact Assessment for the Test, Trace, Protect strategy provides further detail on the rationale behind the joint controller status of partners. Each party is responsible for compliance with data protection legislation, as set out in this agreement. The parties agree that personal data processed and shared in line with this agreement will be used only for the specific purpose(s) set out in this agreement and its schedules.

1.7 This agreement does not replace any contractual arrangements or any requirement for data processing agreements with third party suppliers of any goods and services required to deliver the Test, Trace, Protect strategy. Where such processing agreements are in place, they are referenced in the attached schedules.

1.8 Parties to this agreement will ensure that all personal data shared is adequate, relevant, accurate, up to date and necessary to meet the stated purpose(s).

1.9 Parties to this agreement shall ensure any subsequent processing of shared or jointly processed data (for example, for reporting purposes) complies with data protection legislation.

1.10 As joint controllers, parties to this agreement may engage the services of other controllers or processors to deliver the services and activity described in this agreement. The responsibility for ensuring adequate measures are in place to ensure compliance with data protection legislation is as follows:

1.10.1 Where two or more parties to this agreement collaborate or share resources, they shall ensure any processing complies with data protection legislation.

1.10.2 Where a party or parties to this agreement engage a third party, whether controller or processor, they shall ensure any processing complies with data

protection legislation and that any relevant agreements or contracts are in place.

1.11 This agreement applies to the specific arrangements required to deal with the COVID-19 outbreak only. This agreement will cease to have effect when the need to share information for this purpose end. Any intention to continue sharing in line with this agreement, as a business as usual activity, may be subject to a Data Protection Impact Assessment, which will include the identification of valid lawful bases under data protection legislation and the completion of an Information Sharing Protocol, if required.

2 Purpose of Disclosure

2.1 Personal data is disclosed and shared for the following purposes:

- **Testing** for COVID-19 is vital for:
    - Diagnosing the disease to help with treatment and care.
    - Population health surveillance, so that the spread of the disease can be understood and clusters and hot spots identified.
    - Contact tracing, to control the spread of the disease.
    - Business continuity, enabling key workers to return to work more quickly and safely
    - Knowing who has had the infection in the past, when antibody testing is available.

- **Contact tracing** is a tried and tested method of controlling the spread of infectious diseases. It will also help develop the understanding of how the disease is passed from person to person.

  At a national level, Welsh Government will lead and provide strategic direction, including using developing scientific advice to inform the national response. Public Health Wales will provide national co-ordination, expert advice and support on contact tracing methods and priorities, which will ensure there are robust all-Wales standards and comprehensive guidance for how contact tracing should operate.

  NHS Wales Informatics Service will ensure that there is a single digital platform for contact tracing across Wales. This will allow people to simply and quickly report their contacts, supporting contact tracing teams to work effectively, and providing real time intelligence across the whole of Wales on the coverage of the disease, how quickly it is spreading, and where there are hotspots of infection.

  Contact tracing will be delivered regionally with Local Health Boards and Local Authorities working in partnership along with other public services to deploy contact tracing teams who understand the local context. This will help to speed up contact tracing activity, and to identify new trends or local clusters of the disease as early as possible.

  Alongside this work, there is an intention to have a UK-wide digital app which people can activate on smartphones to anonymously track when two devices using the app

are close together. This ‘proximity tracking’ is different to contact tracing, because it does not record any personal or location details. But it can help manage the spread of the disease, for example as an early warning system which works more quickly than contact tracing, and by sending an anonymous alert to strangers who would not be reported through contact tracing.

- **Protecting.** Contact tracing is not an end in itself. It enables individuals to take the right steps to protect their families, friends and their community by self-isolating. Self-isolating means as far as possible maintaining distance from other family members, not leaving the house for exercise or work and not visiting the shops for food or other essential items.

  Contact tracing means people may be asked to self-isolate multiple times. The more often people come into contact with others, the more likely it is that they will be required to self-isolate. We recognise the strain that this may place on individuals and their families if they are having to isolate on numerous occasions. While they are self-isolating, some people may need help to get food or medicine. Some people may need ongoing care or help in response to their mental health or physical support needs. This may require the sharing of information between various stakeholders.

3 The information sharing partner organisations

3.1 Organisations and single points of contact are shown at Appendix A.

4 Lawful basis

Table 1 - Article 6, GDPR - Personal Data

Condition for processing	Check box / Notes
Task carried out in the public interest or in the exercise of official authority – Art 6(1)(e)	☒ Section 8(c) of the Data Protection Act sets out that such a task must be necessary for the performance of a function conferred on a person by an enactment or rule of law. **Local Authorities** Public Health (Control of Disease) Act 1984, amended by the Health & Social Care Act 2008. Part 2A of the 1984 Act enables the Welsh Ministers, by regulations, to make law for the purpose of preventing, protecting against, and controlling or providing a public health response to the incidence or spread of infection or contamination in Wales. Subordinate legislation, including the Health Protection (Notification) (Wales) Regulations 2010 and the Health Protection (Local Authority Powers) (Wales) Regulations 2010 specify the public health responsibilities of Local Authorities. The Coronavirus Act 2000, Schedule 21, paragraphs 54(2)(b) and 58(3)(a) provide powers for a ‘public health officer’ to collect and share personal data of infectious or potentially infectious individuals.

	Public Health Wales PHW was established under theThe Public Health Wales National Health Service Trust (Establishment) Order 2009. Its functions include the provision and management of a range of public health, health protection, healthcare improvement, health advisory, child protection and microbiological laboratory services and services relating to the surveillance, prevention and control of communicable diseases. **Health Boards** Pursuant to Section 3 of the National Health Service (Wales) Act 2006 the Welsh Ministers have a statutory duty to arrange for the provision of healthcare services to the extent that it considers necessary to meet all reasonable requirements. Pursuant to the Local Health Board (Directed Functions) (Wales) Regulations 2009, the duty under Section 3 of the 2006 Act has been delegated to the Local Health Boards. Such delegated functions include (not limited to) (i) the provision of services outside of Wales (Section 6(2)(c)), providing other services or facilities required for the diagnosis and treatment of illness (Section 3(1)(f)). **NHS Wales Informatics Service** Pursuant to the Velindre National Health Service Trust (Establishment) Amendment Order 2012, the functions of the Velindre NHS Trust were amended so as to include "the managing and providing services relating to information technology, health information, telecommunications and prescribing and dispensing". **Welsh Ambulance Services NHS Trust** Detail to be added here

Table 2 - Article 9, GDPR - Special Categories of Personal Data

Legal basis	Checkbox / Notes
Provision of preventative or occupational medicine, health or social care or treatment, or the management of health or social care systems – Art 9(2)(h)	☒ The Data Protection Act 2018, Schedule 1, Part 1, paragraphs 2(1), (2) & (3) confirm that this condition is met if processing is necessary for health and social care purposes and is carried out by a health or social work professional, or another person who in the circumstances owes a duty of confidentiality.
Public health - Art 9(2)(i)	The Data Protection Act 2018, Schedule 1, Part 1, paragraphs 3(a) & (b) confirm that this condition is met if processing is necessary for the reasons of public interest in the areas of public health and is carried out under the responsibility of a health professional or another person who in the circumstances owes a duty of confidentiality. The legislation described in table 1, above clarifies the respective duties and powers of the partners to this agreement. In the circumstances, there is a clear public interest in processing

	personal data for the purposes described in this agreement and its schedules.

Table 3 – other legal considerations

Other legal considerations	Checkbox / Notes
The common law duty of confidence	The Secretary of State for Health and Social Care has issued four notices under the Health Service (Control of Patient Information) Regulations 2002 ("the COPI regs") to all organisations providing health services, General Practices, and Local Authorities. These notices provide organisations a legal way of setting aside the common law duty of confidence for processing patient information in response to the Covid-19 outbreak, where other lawful basis do not adequately set aside the common law. On 1 April 2020, Welsh Government issued a notice to all organisations providing health services, General Practices and Local Authorities asking them to consider making use of these provisions to process confidential information where it is required solely for the purpose of a response to COVID-19. This means that while the above notices are in force, patient consent or another legal gateway is not required to meet this common law duty. This applies to processing required to deal with the response to COVID-19 only.

5 Data to be Disclosed

5.1 The personal data disclosed and processed is referenced in the schedules to this agreement. It will be limited to the data required to deliver an effective Test, Trace, Protect programme.

6 Information Security

6.1 Parties to this agreement will ensure that the confidentiality, integrity and availability of personal data will be maintained, in line with the schedules to this agreement.

7 Data Subjects' Rights and Requests for Information

7.1 Parties to this agreement will ensure that data subjects are informed how and why their personal data will be processed and who it is shared with (the Right to be Informed). A tiered approach will be adopted. This will include national level fair processing information, where appropriate, supplemented by local information that will identify the partners (with contact points) involved in specific elements, such contact tracing service hubs. Existing privacy notices will be reviewed and updated, where

required, to reflect any additional processing of personal data required to implement the Test, Trace, Protect strategy.

7.2 Allowing data subjects to exercise their rights, including the right of access, is a core element of compliance with data protection legislation. Parties to this agreement will need to be flexible in their approach, in line with the schedules to this agreement

7.3 The principles set out in the schedules should be applied to other requests for information; for example, those made under the provisions of the Freedom of Information Act 2000.

8 Personal data breaches and complaints

8.1 Parties to this agreement will ensure that statutory obligations are met in relation managing, mitigating, investigating and reporting any personal data breach, in accordance with the schedules to this agreement.

8.2 Parties to this agreement will handle any complaints in line with the schedules to this agreement.

9 Escalation of risks and issues

9.1 Parties to this agreement will escalate operational and technical risks and issues via agreed routes, as set out in the schedules to this agreement.

10 Review

10.1 This is a time limited agreement and will be reviewed every six months or sooner if the status of the COVID-19 response is changed or if there are changes to legislation or regulations that impact on the processing described. The individuals and organisations responsible for ensuring this temporary agreement is reviewed are:

Data Protection Officer, Public Health Wales

Data Protection Officer, NHS Wales Informatics Service

The above individual(s) shall ensure that partners are consulted regarding proposed changes.

11 Agreement Signature **(each party shall sign a copy and email acceptance to Public Health Wales)**

Organisation	
Name	
Position	
Date	
Signature	

12 Appendix A – Parties to the agreement (master copy to be maintained by PHW)

All organisations that have signed this Joint Controller Agreement are listed below. Owing to the complexities of the process and the number of organisations involved, formal acceptance of the agreement is noted separately and held by the Data Protection Officer in Public Health Wales.

Information Sharing Partner Organisations	Owner / Point of contact

13 Schedules

The following schedules are attached to this agreement:

Schedule 1 – the provision of testing to key workers, their households and other citizens.

Schedule 2 – implementation of a contact tracing approach that includes the delivery of regional

Schedule 3 – protecting and supporting Welsh citizens who need to self-isolate to help as part of the protect element of the strategy.

Schedule 4 – responsibilities for General Data Protection Regulation compliance

COVID-19 Joint Controller Agreement

Test, Trace, Protect

Schedule 1 – Test

Description

This schedule describes how information is shared to deliver testing as part of the Test, Trace, Protect strategy.

There are several entry points for testing of citizens of Wales. A detailed process document is embedded below (as at 16 June 2020).

NHS Wales coronavirus testing

A. Members of the public can book a home testing kit via an online portal. NHS England is the Data Controller for this pathway and holds the contract with the third parties involved. NHS Digital and Public Health Wales (PHW) are entering into an agreement, using the NHS Wales Informatics Service (NWIS) as a processor, to allow cross border data flows. This will be incorporated into existing arrangements between PHW and NWIS.

B. Critical workers (not Health and Social care key workers) can book a test directly for them and members of their household with a Community Testing Unit (CTU), Mobile Testing Unit (MTU) or via the home testing pathway. Other testing pathways, such as those managed by third parties, are not included in this schedule.

C. Health and social care key workers can book a test for them and members of their household with a CTU or MTU. This is managed via Local Contact Centres who liaise with the relevant CTU or MTU.

D. It is an ambition that the **national contact tracing system (**described in schedule 2 to this agreement) will allow the central booking of tests but this will not be available on the launch of the system.

E. Onsite, point of care, **antibody testing** (not currently referenced in the process flow diagram) is to be initially delivered by healthcare staff visiting schools and care homes. Lists of individuals to be tested will be provided by the respective site and will be uploaded to a web app developed and hosted by NWIS. The web app will allow health workers conducting tests to manage patient lists and will generate a bar code that can be used to manage test results. NB this web app is specifically for onsite antibody testing and is separate from the

proximity app being developed by NHSX and the Department of Health and Social Care in England.

Personal data to be provided

Demographic data

- Pathways A & B: The personal data required to book a test via the online portal provided by NHS England is provided directly by individuals.
- Pathway C: Data required to book a test is gathered from individuals by the Local Contact Centre and transferred to the appropriate CTU or MTU.
- Pathway D: TBC
- Pathway E: Sites will provide lists of individuals to the respective Health Board, which will liaise with NWIS to allow lists and sites to be uploaded to the web app that facilitates lists management and (in time) results be entered by the health worker conducting the test.

The Master Patient Index (MPI) is used to verify demographic details prior to testing at CTUs, MTUs and onsite antibody testing. This allows the identity of individuals and their NHS number to be verified for the purposes of accuracy and efficiency (eg the creation of bar codes that allows laboratories to associate results to an individual's health record).

Test results

Tests conducted by CTUs, MTUS and onsite antibody tests are processed by Welsh laboratories and are entered into the Welsh Laboratory Information System (WLIMS)

Home tests are processed by non-Welsh laboratories are repatriated to NHS Wales systems via a secure application to application, MESH mailbox. This allows results to be integrated with WLIMS.

WLIMS allow subsequent flows of data:

- Back to the digital app; for those citizens have downloaded it and indicated they wish to have the results through the app (by providing the relevant code). This remains an ambition. See schedule 3.
- To the Welsh Results Reporting System (WRRS) which stores the results and allows them to be viewed in secondary care through Welsh Clinical Portal (WCP) and by GPs through the GP Test Requesting/Reporting (GPTR) application.
- To the COVID-19 data hub (https://nwis.nhs.wales/information-services/covid-19-data-hub/).
- To the Welsh national contact tracing system (see schedule 2).

Retention

Personal data shall be retained in NHS Wales systems and applications in line with the appropriate retention periods applied to the relevant record types.

Retention for personal data processed outside NHS Wales systems and applications will relate to operational records that need to be kept for legal compliance*, or that have a limited life as part of an operational activity. These records will be retained for seven years (the current year plus six financial years).

Records will not be kept after the retention period unless:

- The record is the subject of live litigation or a request for information. In these circumstances, destruction should be delayed until the litigation is complete or the relevant complaint procedure has been exhausted, at which time a new trigger point and retention period is created.
- The record has long-term value for each controller's statutory functions.
- The record has been or should be selected for permanent preservation.

*the whole or part of the record may be extrapolated in order to preserve health and social care activity as part of a Welsh residents Health & Social Care Record. Retention values in these circumstances will be different from those described for operational use.

Escalation points

For matters relating to NHS Wales systems, applications and infrastructure, including data flows to, from and between such systems and applications; the Information Governance Team of NWIS.

For operational matters regarding testing; the Information Governance Team of PHW.

Schedule 2 – Trace

Description

This schedule describes how information is shared to deliver the contract tracing aspect of the Test, Trace, Protect strategy.

Contact tracing services

Contact tracing will be implemented through regional contact tracing services provided by Local Health Boards and Local Authorities, who will engage the staff undertaking the contact tracing and manage those services. Contact tracing will be conducted, and personal data captured and recorded, in line with guidelines provided by Public Health Wales (PHW). Local Health Boards and Local Authorities are responsible for the conduct of the staff delivering services, which includes ensuring they receive appropriate data protection training, are aware of their responsibilities when processing personal and confidential data, and that they appropriately access and use the national contract tracing system.

The national digital solution

A national digital solution ('the national contact tracing system'), based on a CRM system provided by Microsoft supports the contact tracing approach. NHS Wales Informatics Service (NWIS) has purchased the system and holds the contract with Microsoft, which is a processor.

The national digital solution will take an iterative approach. The first version will facilitate contact tracing for positive test results, with subsequent versions allowing for contact tracing of symptomatic individuals and the development of additional functionality.

Requirements for the system are based on the guidelines provided by Public Health Wales (PHW). NWIS provides project support for the development of the national contact tracing system and the integration of existing national systems. NWIS is responsible for undertaking a Data Protection Impact Assessment for the system.

Personal data to be processed

Inputs from national systems:

- **The Welsh Laboratory Information System (WLIMS)** (hosted by NWIS – for the purposes of this agreement, NWIS has controller responsibilities for the extract provided to the national contact tracing system. Once in the system, joint controller responsibilities apply) – provides a feed of COVID-19 test results to the national contact tracing system.

- **The enterprise Master Patient Index (MPI)** (hosted in the NHS Wales Infrastructure - for the purposes of this agreement, NWIS has controller responsibilities for the integration with the national contract tracing system. Once in the system, joint controller responsibilities apply) – provides a 'gold standard' of demographic data taken from national health systems. A cache of the MPI within the NHS Wales infrastructure will be used for the purposes of updating and allowing queries from the national contact tracing system.

Inputs from contact tracing services:

- Staff will gather and record personal data on the national contact tracing system in line with the guidance provided by PHW and instructions from Local Health Boards and Local Authorities managing the services.
- It is the responsibility of Local Authority TTP teams to accurately identify contacts and record in the national system.

Other inputs

- Information may be received from other public health agencies – for example Public Health England – via PHW.

Outputs:

- Data, including personal data, will be used for reporting, which allow the analysis of, for example, patient pathways.
- Reports required by PHW will be taken from the national contact tracing system. Reports will be anonymised unless identifiable data is required to fulfil a purpose associated with the Test, Trace, Protect strategy. Any organisation taking or receiving a report or extract from the system is responsible for the security, integrity and appropriate retention and destruction of that information.
- Information will be shared cross border – for example, where individuals have been in transit from Wales to England, or other countries, or been in contact with individuals who have crossed borders and administrative boundaries – as determined by PHW.

Joint controllers

All partners listed below are joint controllers for the purposes described in this schedule.

- Public Health Wales
- NHS Wales Informatics Service (hosted by Velindre University NHS Trust)
- Welsh Ambulance Services NHS Trust (WAST)
- Partners involved in the delivery of regional contact tracing services:

Cardiff and Vale	**North Wales**
Cardiff and Vale University Health Board The City of Cardiff Council The Value of Glamorgan Council	Betsi Cadwaladr University Health Board Ilse of Anglesey County Council Conwy County Borough Council Denbighshire County Council Flintshire County Council Gwynedd County Council Wrexham County Borough Council

Powys Powys Teaching Health Board Powys County Council	**Gwent** Aneurin Bevan University Health Board Blaenau Gwent County Borough Council Caerphilly County Borough Council Monmouthshire County Council Newport City Council Torfaen Newport City Council
Swansea Bay Swansea Bay University Health Board City and County of Swansea Neath Port Talbot Council	**Hywel Dda** Hywel Dda University Health Board Carmarthenshire County Council Ceredigion County Council Pembrokeshire County Council
Cwm Taf Morgannwg Cwm Taf Morgannwg University Health Board Bridgend County Borough Council Merthyr Tydfil County Borough Council Rhondda Cynon Taf County Borough Council	

Retention

Personal data shall be retained in the national contact tracing system in line with the terms outlined in the contract. NWIS is responsible for ensuring the supplier meets its contracted responsibilities, including the exit strategy.

Retention will relate to operational records that need to be kept for legal compliance*, or that have a limited life as part of an operational activity. These records will be retained for seven years (the current year plus six financial years).

Records will not be kept after the retention period unless:

- The record is the subject of live litigation or a request for information. In these circumstances, destruction should be delayed until the litigation is complete or the relevant complaint procedure has been exhausted, at which time a new trigger point and retention period is created.
- The record has long-term value for each controller's statutory functions.
- The record has been or should be selected for permanent preservation

*the whole or part of the record may be extrapolated in order to preserve health and social care activity as part of a Welsh residents Health & Social Care Record - Retention values in these circumstances will be different from those described for operational use.

Escalation

For operational matters regarding contact tracing; the Test, Trace and Protect team of the relevant local authority.

Operational risks and issues should be escalated through regional leads who will liaise with national leads, as required.

Risks and issue associated with the technical components should be escalated through the agreement service management arrangements.

Schedule 3 – Protect

Description

This schedule describes the sharing of personal data required to protect and support those who need to self-isolate, including those who are vulnerable and need to take additional steps to shield themselves from infection, those who test positive and those who are advised to self-isolate by contact tracing services.

Activity may be added to this schedule as the contact tracing approach matures.

Activity 1 – The NHS COVID-19 App

Work is ongoing to realise the ambition for a UK-wide mobile phone application to help slow or stop the epidemic.

Test, Trace, Protect

Schedule 4 – GDPR Responsibilities

Description

This schedule describes the responsibilities each party is accepting under GDPR. By entering into a Joint Controller Agreement, each party understands that data subjects may exercise their rights in respect of and against each of the controllers and each controller will be liable for the damage caused by processing which infringes GDPR. Controllers shall be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage. Defining the responsibilities aims to protect each party from claims being made against all controllers.

Table of Responsibilities

Article	Description	Public Health Wales (PHW)	NWIS	Health Boards and WAST	LA
5 (1) (a)	Lawful, fairly and transparent	Identification of the lawful basis for processing personal data, in compliance with Article 6 & 9. Development and approval of a national privacy notice. Consult partners prior to amending the national privacy notice. Ensure national privacy notice is	Make the national privacy notice accessible to the public when using any online system.	Agree to the lawful basis for processing personal data, in compliance with Article 6 & 9. Review amendments to the national privacy notice and provide feedback. Publish link to the national privacy notice on HB website.	Agree to the lawful basis for processing personal data, in compliance with Article 6 & 9. Review amendments to the national privacy notice and provide feedback. Publish link to the national privacy notice on LA website.

		available to partners for communication at the point of data collection.			Develop a local privacy notice when required.
5 (1) (b)	Specified, explicit and legitimate purposes	Define the agreed purposes. Approve or reject requests from partners to use the data for secondary purposes.		Process the data for the agreed purposes only.	Process the data for the agreed purposes only.
5 (1) (c)	Adequate, relevant and limited to what is necessary	Decide what personally identifiable data is held within the national system. Define the data fields within the national system. Develop scripts for use by the contact tracers and contact advisors.	Develop a national system that only holds adequate and relevant personal data. In consultation with other stakeholders, define what sources of information are used. Decide what data matching is undertaken with other sources of data.	Only record information in the system that is necessary for the purposes.	Only record information in the system that is necessary for the purposes.
5 (1) (d)	Accurate and up to date		The accuracy of demographic data	Accuracy of all information entered	Accuracy of all information entered

			provided to the national CRM system by the MPI. Accurately importing test result data from the NHS England infrastructure into the NHS Wales infrastructure and on to the national contact tracing system. Not the accuracy of test results.	into the system by HB staff. Keeping cases assigned to the HB up to date.	into the system by LA staff. Keeping cases assigned to the LA up to date.
5 (1) (e)	Kept for no longer than necessary	Define the data retention policy. Apply the retention policy to any data held locally.	Apply the data retention policy to data in national systems.	Apply the retention policy to any data held locally.	Apply the retention policy to any data held locally.
5 (1) (f)	Technical and organisational measures	GDPR staff training. Any activity attributed to a PHW user account. Security of devices used by PHW.	Ensure the control measures detailed in the CRM DPIA are applied to protect confidentiality, integrity and	GDPR staff training. Any activity attributed to a HB user account. Security of devices used by HB.	GDPR staff training. Any activity attributed to a LA user account.

			availability of the system. GDPR staff training. Any activity attributed to a NWIS user account. Security of devices used by NWIS.		Security of devices used by LA.
5 (2)	Demonstrate compliance	Be able to demonstrate compliance with responsibilities under this agreement.	Be able to demonstrate compliance with responsibilities under this agreement.	Be able to demonstrate compliance with responsibilities under this agreement.	Be able to demonstrate compliance with responsibilities under this agreement.
13	Privacy Notice	Develop and approve the national privacy notice. Consult with partners prior to amending national privacy notice. Publishing the national privacy notice. Ensure all telephone scripts include	Ensure national privacy notice is included on all public facing systems.	Provide feedback on any draft amendments to national privacy notice. Publish the link to the national privacy notice on the HB website. Ensure all staff read out scripts referring to national privacy notice.	Provide feedback on any draft amendments to national privacy notice. Publish the link to the national privacy notice on the LA website. Ensure all staff read out scripts referring to national privacy notice.

		reference to the national privacy notice.		Develop local privacy notice when authorised by PHW to use the data for a secondary purpose.	Develop local privacy notice when authorised by PHW to use the data for a secondary purpose.
15	Right of Access	Respond to right of access requests for non-Welsh residents.	Provide LA's the ability to extract from the CRM all data in a machine readable format.		Respond to right of access requests for residents of the LA area. Transfer any requests received that fall outside of the LA area to the appropriate partner and notify the data subject.
16	Right to Rectification	Respond to all requests for rectification for non-Welsh residents.	Respond to all requests for rectification that relate to inaccurate data, other than any data input by the LA.		Respond to all requests for rectification for residents of the LA area. Transfer any requests received that fall outside of the LA area to the appropriate partner and notify the data subject.

17	Right to Erasure	Respond to all requests under right to erasure.			
18	Right to Restriction	Respond to all requests under right to restriction.			
24	Responsibilities of the controller	Comply with the joint data controller agreement. Maintain up to date Data Protection policies that cover TTP processing activities.	Comply with the joint data controller agreement. Maintain up to date Data Protection policies that cover TTP processing activities.	Comply with the joint data controller agreement. Maintain up to date Data Protection policies that cover TTP processing activities.	Comply with the joint data controller agreement. Maintain up to date Data Protection policies that cover TTP processing activities.
25	Data Protection by design and by default	Define what personal data are processed.	Design and implement technical controls to protect personal data within the CRM.		
26	Joint Controllers	Agree to comply with responsibilities set up in the joint controller agreement.	Agree to comply with responsibilities set up in the joint controller agreement.	Agree to comply with responsibilities set up in the joint controller agreement.	Agree to comply with responsibilities set up in the joint controller agreement.
28	Processors	Ensure adequate contractual arrangements are in place for processors engaged by PHW.	Ensure adequate contractual arrangements are in place for processors engaged by NWIS.	Ensure adequate contractual arrangements are in place for processors engaged by HB.	Ensure adequate contractual arrangements are in place for processors engaged by LA.

		Take full responsibility for all lawful actions taken by processors engaged by PHW.	Take full responsibility for all lawful actions taken by processors engaged by NWIS.	Take full responsibility for all lawful actions taken by processors engaged by HB.	Take full responsibility for all lawful actions taken by processors engaged by LA.
30	Records of Processing Activities	Maintain a record of processing activities under its responsibilities.	Maintain a record of processing activities under its responsibilities.	Maintain a record of processing activities under its responsibilities.	Maintain a record of processing activities under its responsibilities.
31	Cooperation with the ICO	Cooperate with the ICO on all matters.	Cooperate with the ICO on all matters.	Cooperate with the ICO on all matters.	Cooperate with the ICO on all matters.
32	Security of Processing	All activity associated with PHW user accounts. Security of devices used by PHW.	Ensure the control measures detailed in the CRM DPIA are applied to protect confidentiality, integrity and availability of the system. All activity associated with NWIS user accounts. Security of devices used by NWIS.	All activity associated with HB user accounts. Security of devices used by HB.	All activity associated with LA user accounts. Security of devices used by LA.
33	Notification of personal data breaches to ICO	Manage personal data breaches in line with own internal procedures.	Manage personal data breaches in line with own	Manage personal data breaches in line with own internal procedures.	Manage personal data breaches in line with own

		Inform the ICO, where necessary, of personal data breaches following a breach of security in an area of responsibility. Inform all other joint controllers of personal data breaches.	internal procedures. Inform the ICO, where necessary, of personal data breaches following a breach of security in an area of responsibility. Inform all other joint controllers of personal data breaches.	Inform the ICO, where necessary, of personal data breaches following a breach of security in an area of responsibility. Inform all other joint controllers of personal data breaches.	internal procedures. Inform the ICO, where necessary, of personal data breaches following a breach of security in an area of responsibility. Inform all other joint controllers of personal data breaches.
34	Communication of personal data breach to data subject	Inform data subjects, where necessary, of personal data breaches.	Inform data subjects, where necessary, of personal data breaches.	Inform data subjects, where necessary, of personal data breaches.	Inform data subjects, where necessary, of personal data breaches.
35	Data Protection Impact Assessment	Development and maintenance of a DPIA for the TTP scheme. Consult with partners prior to amending a DPIA.	Development and maintenance of a DPIA for the national system.	Provide feedback when consulted.	Provide feedback when consulted.
36	Prior Consultation	Consult with the ICO prior to processing. Make all ICO advice received available to partners.			

37	Data Protection Officers	Appointment of a DPO. Engage partner DPO's directly on all data protection matters. Consult partner DPO as required by this agreement.		Appointment of a DPO. DPO to fully engage with the project. DPO to raise any issues with SIRO and/or Chief Executive as appropriate.	Appointment of a DPO. DPO to fully engage with the project. DPO to raise any issues with SIRO and/or Chief Executive as appropriate.
44	International Transfers	Ensure that any processors engaged hold the data in accordance with the requirements of GDPR.	Ensure that all parts of the national system and data reside in the UK. Ensure that any processors engaged hold the data in accordance with the requirements of GDPR.	Ensure that any processors engaged hold the data in accordance with the requirements of GDPR.	Ensure that any processors engaged hold the data in accordance with the requirements of GDPR.
82	Right to compensation and liability	Accept responsibility for all compensation claims as a result of its own non-adherence to this agreement.	Accept responsibility for all compensation claims as a result of its own non-adherence to this agreement.	Accept responsibility for all compensation claims as a result of its own non-adherence to this agreement.	Accept responsibility for all compensation claims as a result of its own non-adherence to this agreement.

89	Archiving	Accepts responsibility for processing for archiving purposes.			
DPA2018	Information requests under Schedule 2	Respond to information requests received by third parties in line with own internal procedures.	Respond to information requests received by third parties in line with own internal procedures.	Respond to information requests received by third parties in line with own internal procedures.	Respond to information requests received by third parties in line with own internal procedures.