This deed is dated 11/01/2021

DEED OF AGREEMENT FOR DATA SHARING BETWEEN

THE REGIONAL AGENCY FOR PUBLIC HEALTH AND SOCIAL WELL-BEING (KNOWN AS THE PUBLIC HEALTH AGENCY) NORTHERN IRELAND

And

HEALTH SERVICE EXECUTIVE (HSE)

For

COVID-19 Cross-border Contact Tracing System (CTS)

1.	**Parties to this Agreement**	
	The Public Health Agency Address 4th Floor, 12-22, Linenhall Street, Belfast, BT2 8BS Phone: I&S Email address: Pha.dutyroom@hscni.net	Health Service Executive Dr Steeven's Hospital, Steevens Lane, Dublin 8, D08 W2A8. Phone: I&S Email address: ncdhp@hpsc.ie
2.	**Introduction** 2.1 For the purpose of this Deed of Agreement for Data Sharing (the "Agreement"), the Northern Ireland Public Health Agency will be referred to as the PHA and the Republic of Ireland Health Service Executive will be referred to as the HSE (together the "Parties" and each a "Party"). 2.2 This Agreement constitutes the legally binding and enforceable instrument between public bodies pursuant to Article 46 (2) (a) of GDPR. 2.3 This Agreement sets out the information sharing arrangement between the PHA and the HSE that governs the exchange of information between the Parties. For context, this "information" is defined as a collective set of Personal Data and/or facts that when shared between the Parties through this Agreement can support the Parties to better deliver their respective organisations' objectives and/or functions. 2.4 The Processing activities set out in this Agreement which require the sharing of Personal Data between the Parties relate to COVID 19 Contact Tracing, and have been agreed to ensure the sharing of Personal Data to assist the PHA and the HSE in limiting the spread of COVID 19 through such Contact Tracing in compliance with Data Protection Legislation. 2.5 Given the propensity for cross border travel between NI and ROI, particularly in border counties, this Agreement allows for the safe sharing of Personal Data in a number of categories. These include (but are not exclusive to) travel, employment, leisure or sporting events and attendance at educational settings. Personal Data shared will only be relevant to individuals who are Index Cases or potential contacts of confirmed cases of Covid19.	

2.6 The Personal Data shared by the PHA Health Protection Team will be specific to contacts residing in RoI and the Personal Data shared by the HSE (including the Health Protection Surveillance Centre (HPSC)) will be specific to contacts residing in Northern Ireland.

2.7 The aim of the Agreement is to set clear guidelines to follow when sharing Personal Data and to ensure that Personal Data is shared in accordance with Data Protection Legislation.

2.7.1 This Agreement aims to;

- set out the high-level principles that will govern the sharing of Personal Data between the Parties;
- describe the processes, structures and roles that will support the exchange of Personal Data between the PHA and the HSE;
- set out the legal responsibilities which apply to disclosure and use of Personal Data having regard to Data Protection Legislation;
- describe the Personal Data security procedures necessary to ensure compliance with Data Protection Legislation and any other specific security requirements or supplementary measures required;
- describe the process for managing Data Breaches; and
- describe the process for monitoring and reviewing the use of this Agreement.

2.8 The legal basis for sharing Personal Data is set out in section 7 of this Agreement.

2.9 The PHA was established as the Regional Agency for Public Health & Social Well-being ("the Regional Agency") under Section 12(1) of the Health and Social Care (Reform) Act (Northern Ireland) 2009 ("2009 Act"). The 2009 Act sets out the PHA Health Protection function, including that "The health protection functions are the protection of the community (or any part of the community) against communicable disease in particular by the prevention or control of such disease." In respect of COVID 19, this means that the PHA will operate the Contact Tracing Service to help break the chain of transmission of the COVID 19 virus, as required by the Department of Health, in line with the DOH 'COVID 19 Test, Trace and Protect Strategy: Saving lives by minimizing SARS-CoV2 transmission in the community in Northern Ireland', 27 May 2020.

2.10 The PHA Health Protection function is also governed by the provisions of the Public Health Act (Northern Ireland) 1967 and the Coronavirus Act 2020 and associated Regulations.

2.11 The HSE is a corporate body with perpetual succession established by the Health Act 2004 as the single body with statutory responsibility for the management and delivery of health and personal social services in the

Republic of Ireland, which has its principal administrative offices at Dr Steeven's Hospital, Steevens Lane, Dublin 8, D08 W2A8. The objective of the HSE is to use the resources available to it in the most beneficial, effective and efficient manner to improve, promote and protect the health and welfare of the public.

2.12 Both the PHA and the HSE have a statutory responsibility for the health and wellbeing of the population they serve. In light of these statutory obligations, it is important to emphasise that the current collaborative working and data sharing agreements that exist between both organisations will be maintained from 1 January 2021 following the end of the transition period and the UK becoming a third country for data protection purposes.

2.13 Personal Data will be shared on both adults and children as necessary for the purpose of Contact Tracing. Personal Data is collected from the individuals who have tested positive or the individuals they have been in contact with during the period of being infectious. The data collected on all contacts will be the minimum necessary to allow these people to be contacted. Where the Personal Data relates individuals under the age of 16 or without capacity in ROI (i.e. a child or a vulnerable adult), then such Personal Data may be collected through their representative or proxy and communications by the HSE in respect of that Personal Data will be with the representative or proxy as applicable. For the purpose of this Agreement where Personal Data relates to individuals under the age of 16 or without capacity in NI, then such Personal Data may be collected through their representative or proxy and communications by the PHA in respect of that Personal Data will be with the representative or proxy as applicable.

2.14 The PHA and the HSE are committed to maintaining regular contact, including through the following regular cross border meetings and communication:

- Weekly teleconference, RoI border county, HPSC and NI representation.
- Daily RoI Border County and NI phone call.
- Fortnightly track and Trace teleconference-Chaired by Department of Health RoI. HPSC, HSE DPH and Contact Tracing Centre (CTC) and PHA and CTC representations
- Weekly Health Protection-Cross border Health Protection committee chaired by HP leads in RoI and NI

This will allow for

- better management of cross border outbreaks, or raise issues/areas of concern
- Exchange of "knowledge behind the data" and ensure we have a regular channel of open communication between RoI and NI.

	- Operational decisions around establishing Incident Management Teams in cross border clusters/outbreaks 2.15 The PHA is the Data Controller, for the personal data held by the PHA COVID 19 Contact Tracing Programme, under the Data Protection Act 2018 (DPA 2018) UK. The HSE is a Data Controller for the personal data held by HPSC and RoI Public Health departments under the Data Protection Act 2018 (DPA 2018) ROI. The Parties shall be considered independent Data Controllers for any Personal Data and/or Special Categories of Personal Data shared with each other under this Agreement. It is important to emphasise that the current collaborative working between the PHA and HSE will be maintained and the purpose of sharing Personal Data is to reduce the risk or the spread of COVID-19. 2.16 When a Party shares Personal Data and/or Special Categories of Personal Data with the other Party, the Party receiving the Personal Data and/or Special Categories of Personal Data shall be considered the Data Controller for that copy of the Personal Data and/or Special Categories of Personal Data which they have received from the other Party. 2.17 There may be limited circumstances where the Parties act as joint controllers or where one Party acts as a data processor for the other Party. In all of these circumstances, the Parties will fully comply with their respective obligations under Data Protection Legislation in respect of the Personal Data. 2.18 Each Party is responsible for complying with their obligations as Data Controllers under the relevant Data Protection Legislation in that jurisdiction. 2.19 The Parties shall co-operate, facilitate and assist each other so that each may comply with their respective obligations under their Data Protection Legislation.
3.	**Purpose & Scope** 3.1 This Agreement is being entered into by the Parties to ensure the sharing of Personal Data to assist the PHA and the HSE in limiting the spread of COVID-19 through Contact Tracing. 3.2 The Personal Data shared under this Agreement is being collected in line with PHA and HSE arrangements to respond to the COVID 19 pandemic. These arrangements are also in line with international measures to respond to COVID 19, as articulated by the WHO and under Articles 23 ('Health measures on arrival and departure'), 44 ('Collaboration and assistance') and 45 ('Treatment of personal data') of the international Health Regulations (IHR) 2005, including arrangements in the RoI (of

particular relevance due to the land border, and the amount of cross-border movement).

3.3 The purpose of the processing of Personal Data is to reduce the risk or the spread of COVID 19 on the island of Ireland by: -

- Identifying and providing appropriate advice to those persons who have tested positive for COVID 19 in one jurisdiction, but reside in the other (Index Cases);
- Identifying and providing appropriate advice to contacts of an Index Case in one jurisdiction where the contact resides in the other jurisdiction.

  (The health protection team of the jurisdiction where the Index Case or the contact resides will make contact to provide the appropriate advice relevant to that jurisdiction.)
- Identifying clusters or outbreaks of infection (that is individuals with confirmed COVID-19 who are linked in time, place or person). If a suspected cluster of COVID-19 , which includes person or place in the other jurisdiction, is identified by the Contact Tracing Service, the;
  - **PHA** Health Protection Team overseeing the service will notify the HSE via password protected email with contact information to a secure email at healthprotectionhpsc@hpsc.ie.
  - **HSE** Health Protection Team overseeing the service will notify the NI PHA via password protected email with contact information to a secure email at NIContacttracing@hscni.net
- **Surveillance;** to control the spread of infectious diseases by bringing together a range of anonymised data about the disease in a timely manner, to inform decisions and actions across both public health systems. This will include understanding the areas of the country which are most affected by an outbreak whether particular groups of people are affected, whether symptoms are getting more severe, when the outbreak might have peaked and helping to predict how the outbreak will progress based on a range of different scenarios. Surveillance data will use the Personal Data to identify cross-border clusters for Covid-19 and will allow better management of cross border outbreaks.

3.4 The Personal Data will be held for the primary purposes of tracing and contacting individuals who have tested positive or been in contact with someone who has tested positive for COVID 19, to give them appropriate advice to help reduce/prevent the further transmission of the virus, and for management of clusters. Identifiable Personal Data is also required for cluster or outbreak management by health protection specialist staff, so that

	appropriate risk assessment and outbreak control measures can be implemented that is specific to the situation. 3.5 The Personal Data is used for the following purposes: • To contact the confirmed case, to provide public health advice, relevant to the jurisdiction where the person resides, and to seek information on others that they have been in contact with; • To contact those who have been in close contact with someone who has tested positive, to give appropriate public health advice, relevant to the jurisdiction where the person resides. • To identify and manage clusters and outbreaks of disease. • Sharing personal information with the PHA and HSE in adherence with the legal regulations in section 7; • Public health surveillance – to identify and manage clusters of disease, identify trends in the COVID 19 disease outbreak and to prevent/control spread; and • Analysis – for reports and the production of official statistics (anonymized data).
4.	**Details of data to be shared and data flows** 4.1 The Parties shall be considered independent Data Controllers for any Personal Data and/or Special Categories of Personal Data shared with each other under this Agreement. 4.2 All citizens in Northern Ireland (NI) and Republic Of Ireland (ROI) with symptoms of COVID19 are entitled to a test. 4.3 Personal Data may be shared with the relevant Health Protection Service (PHA and HSE) where the confirmed case has visited RoI or NI or been in contact with someone who lives in RoI or NI during the period when they have been potentially infectious. The information would be used so that the relevant Health Protection service (PHA and HSE) can initiate contact tracing for the affected individual who lives in NI or RoI as appropriate. 4.4 For the PHA, the source data will come from the PHA Contact Tracing Information System. Please refer to the PHA Data Protection Impact Assessment (DPIA 03/20) for the Contact Tracing Service. 4.5 For the HSE, the information is sourced from the Computerised

Information and Disease Reporting (CIDR) system. CIDR is hosted and operated by the HSE HPSC. CIDR is an information system developed to manage the surveillance and control of infectious diseases in Ireland. CIDR is a shared national information system for the CIDR partners - the former health boards, the Health Protection Surveillance Centre, the Food Safety Authority of Ireland, the Food Safety Promotion Board and the Department of Health. Please refer to the HPSC's "CIDR-Privacy Impact Assessment" for further information. CIDR resides within the HPSC's IT domain, separate from the HSE. The HPSC domain is subject to the controls of the HPSC's Information Security Management Systems (ISMS) and is Certified to the ISO27001 Information Security Standard. This system is subjected to regular external certification audits by an ISO accredited auditing body.

Information is shared in the following way:

Data from NI to RoI:

By email/phone call

Where information about a confirmed case or a close contact who has visited or resides in RoI is received by the PHA, Personal Data for the cases/close contacts will be sent to the HPSC to the designated email address (healthprotection@hpsc.ie). The information will be shared via an encrypted password protected file. Any urgent issues that require public health action out of hours are shared directly by phone with the doctor on call for health protection (phone number in Data Flow section 5).

Data from RoI to NI

By email/phone call
Where information about a confirmed case or a close contact who has visited or resides in Northern Ireland is communicated to the HPSC via a Contact tracing Centre (CTC) or via a regional Department of Public Health (DPH), the details of the cases/close contacts will be sent to the PHA. The information will be shared via an encrypted password protected file to the designated email address (nicontacttracing@hscni.net) Urgent cases are shared by phone with the consultant on call for health protection (phone number in Data Flow section 5).

Data from both NI and RoI

By teleconference/video call
Information about cases or close contacts or settings where outbreaks occur may be shared by teleconference or by encrypted videoconference in the event of cross border outbreaks. Examples

of encrypted video conferencing platforms include Webex® and Zoom®.

4.6 The Minimum Data Set (MDS) required for this:
Administrative details for those providing the information (name, organisation, position, contact details);

The following Personal Data relating to case/contacts of confirmed COVID 19 cases will be transferred between the Parties during the Term of this agreement:

For cases:

- Case names
- Case date of birth
- Case address including full postcode
- Case telephone number
- Case email
- Case date of onset of symptoms
- Case date of testing
- Case date of test result

For contacts:

- Contact names
- Contact date of birth
- Contact address including postcode
- Contact telephone number
- Contact email

The above MDS is necessary in order to carry out the Health Protection function in PHA and HSE.

4.7 For PHA the names and telephone number of contacts of cases are collected in the initial call made to the case. An automated text message is then sent to the identified close contacts in NI and RoI. This is followed up by passing on the information about the identified close contacts to the HSE to allow them to follow up on close contacts and advise them on self-isolation.

4.8 For PHA information provided by the case, and collected about the contact, for the purposes of contact tracing for COVID 19 will not be used for any purpose that is not linked to COVID 19. The contacts name and contact details will be provided by the case who they have been in contact with. If they have travelled on a flight or a ship with someone who has tested positive their details will be provided by the relevant service provider. The details of the confirmed case will not be shared with the contacts, in accordance with the PHA Privacy Notice for Contact Tracing, accessed via

	link below: https://www.publichealth.hscni.net/covid-19-coronavirus/testing-and-tracing-covid-19/privacy-information 4.9 For HSE Personal Data is protected by the HSE in accordance with the HSE's Privacy Statement which can be accessed via https://www.hse.ie/eng/privacy-statement/. The HSE's COVID-19 specific information notice can be accessed via https://www.hse.ie/eng/gdpr/data-protection-covid-19/. For HSE information provided by the case, and collected about the contact, for the purposes of contact tracing for COVID 19 will not be used for any purpose that is not linked to COVID 19.
5.	**Data Flow Map** Please refer to **Appendix 1a** -for the Standing Operating Procedure (SOP) for COVID 19 information sharing between PHA and HSE. Please refer to **Appendix 1b** – Data Flows for positive cases of COVID-19 and close contacts from RoI to NI and from NI to RoI.
6.	**Personal Data use/Compliance with Article 5 of GDPR and Article 46 of GDPR** 6.1 All Parties will ensure the information shared under this Agreement will only be used for the specific purpose set out in Section 3. Other than as specified in this Agreement, there will be no onward sharing or further Processing of Personal Data beyond the Parties. 6.2 The Parties acknowledge that. Personal Data may require to be shared with other healthcare bodies and professionals, including GPs and hospitals, for the purposes of public health protection and that these are specific and exceptional circumstances under which such data sharing is permitted without prior authorisation, but subject to (i) the use being compatible with the specific purpose set out in Section 3; and (ii) the use having been previously notified to the transferring Party. 6.3 Onward transfers of Personal Data other than as specified above, are only permitted if the transferring Party has given its prior and express authorisation to the transfer and the receiving third party or parties commit to respect the same data protection principles and safeguards as are included in this Agreement including a commitment to provide to Data Subjects the same data protection rights and guarantees as provided for in

	this Agreement. The receiving Party must in these circumstances provide sufficient information on the Personal Data which it intends to transfer/share and the reasons and purposes for which it considers it to be necessary to transfer/share the Personal Data. 6.4 The Parties will ensure that each of them shall comply with the guidance of any relevant regulatory authority on Restricted Transfers to include any additional or supplemental measures required to be taken in the context of any such Restricted Transfers including the requirement to carry out risk assessments and to adopt mitigating measures to ensure essentially equivalent protection for Data Subjects (in particular in respect of the transfer of Shared Personal Data by the HSE to the PHA post-Brexit). 6.5 Where a Restricted Transfer is concerned, the transferring Party's consent to such Restricted Transfer is required. Where such consent has been obtained, the Restricted Transfer may only be made where there are Appropriate Safeguards in place with regard to the rights of Data Subjects (including but not limited to the Standard Contractual Clauses, binding corporate rules, or any other model clauses approved by the DPC or the ICO as the case may be). The Party who is entering into the Appropriate Safeguards with a data importer shall comply with the guidance of any relevant regulatory authority on Restricted Transfers in particular with respect to the use of Standard Contractual Clauses and any additional or supplementary measures required to be taken in the context of any such Restricted Transfers including the requirement to carry out risk assessments and to adopt mitigating measures to ensure essentially equivalent protection for Data Subjects in the jurisdiction of the data importer. 6.6 The transferring Party will keep a record of all notifications from the receiving Party and provide this information to its Supervisory Authority upon request. 6.7 Both Parties will share Personal Data in line with the 7 Data Protection Principles below; - Lawfulness, fairness and transparency: - Purpose limitation: - Data minimization: - Accuracy: - Storage limitation: - Integrity and confidentiality (security): - Accountability:

7.	**Legal Basis for Data Sharing/Compliance with Article 6 and Article 9 of GDPR** **7.1 Article 6(1) of GDPR** 7.1.1 The lawful bases for processing the specified Personal Data under this Agreement is: 7.1.2 Article 6 (1) (e) of GDPR – 'the 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'. 7.1.3 It is acknowledged that some of the Personal Data (health data) to be shared as part of this agreement services will be Special Category Data, as defined in Data Protection Legislation. For the purposes of this Agreement, the following lawful basis for processing is relied upon by the respective Parties. Article 9(2) (i) of GDPR: '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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the Data Subject, in particular professional secrecy'. **7.2 Data Protection** 7.2.1 Personal Data is shared between the PHA and the HSE under the UK and ROI Data Protection Acts 2018 as follows: The Data Protection Act 2018 (DPA 2018) UK – Schedule 1, Part 1 (3) – reasons of public interest in the area of public health: *"This condition is met if the processing—* *(a) is necessary for reasons of public interest in the area of public health, and* *(b) is carried out—* *(i) by or under the responsibility of a health professional, or* *(ii) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.* RoI: Under the Data Protection Act 2018 (DPA 2018) ROI, The data collected by the HSE under the governance of the Departments of Public Health / Medical Officers of Health (MOH), National Clinical Director for Health Protection. The data therefore is collected under Medical Officer

	of Health legislation including: • Health Act 1947 (as amended) • • S.I. No. 390 of 1981 Infectious Diseases Regulations, 1981 (as amended) • S.I. No. 128/1949 - Health (Duties of Officers) Order, 1949 7.2.2 In addition, under the Data Protection Act 2018 (DPA 2018) ROI and GDPR "data concerning health" falls within the definition of Special Category Personal Data and can be processed in situations where necessary to do so for reasons of public health. The legal basis for collecting the data is interpreted as being allowable under GDPR. **7.3 International Health Regulations** 7.3.1 Information is shared between the parties under the International Health Regulations (IHR) 2005 including Articles 23, 44 and 45, which provide the parties with a basis in international law for collecting, collaborating on and sharing Personal Data for Contact Tracing purposes to contact trace close contacts of a person with COVID-19. **7.4 EU Decision 1082/2013/EU** 7.4.1 Both the EU (EU Decision 1082/2013/EU) and the WHO indicate that Contact Tracing and the associated investigation of individuals, who may have been exposed and may be at risk of developing a disease, are important elements of public health investigations. Decision 1082/2013/EU on serious cross-border threats to health lays out in Recital 25: "The occurrence of an event that is linked to serious cross-border threats to health and is likely to have Europe-wide consequences could require the Member States concerned to take particular control or contact-tracing measures in a coordinated manner to identify those persons already contaminated and those persons exposed to risk." Article 9 of EU Decision 1082/2013/EU provides for sharing of contact tracing information between Member States.
8.	**Transparency Obligations** 8.1 The Parties acknowledge the legal rights of Data Subjects and individual members of the public, where appropriate, to access, to rectification, erasure, restriction of processing and to object under Data Protection Legislation (subject access requests). The Parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests submitted under Data Protection Legislation within the time limits imposed.

8.2 The point of contact for each Party is responsible for maintaining a record of individual requests from Data Subjects as to the exercise of their rights the decisions made and any information that was exchanged. Such records will be retained and stored as per respective information retention and disposal policies.

8.3 Individuals can ask for copies of the information that are held on them. Both the PHA and the HSE have an established subject access request (SAR) process to ensure that requests are dealt with promptly and appropriately.

8.4 For the HSE, citizens can access information and service in order to exercise their rights under GDPR and the RoI Data Protection Act 20218 via the HSE's Privacy Statement at: https://www.hse.ie/eng/privacy-statement/ and https://www.hse.ie/eng/gdpr/data-protection-covid-19/

8.5 For the PHA, citizens can access information and service in order to exercise their rights under GDPR and the Data Protection Act 2018 (DPA 2018) UK via the PHA Privacy Notice at:

https://www.publichealth.hscni.net/covid-19-coronavirus/testing-and-tracing-covid-19/privacy-information

8.6 The transparency obligations of the Parties are set out in their respective Privacy Statements referenced above which are incorporated by reference into this Agreement. Data Subjects are entitled to a copy of this Agreement on request.

8.7 Each of the Parties has in place a mechanism to effectively handle, in a timely manner, and resolve, complaints from Data Subjects concerning compliance by the relevant Party with the data protection safeguards set out in this Agreement. Where a Data Subject is not satisfied as to the way in which their complaint is dealt with by the relevant Party or Parties, then in respect of the HSE, the Data Subject can seek redress from the DPC and in the case of the PHA, the Data Subject can seek redress from the ICO, each of which shall have independent oversight in its respective jurisdiction regarding the data sharing arrangements under this Agreement.

8.8 The Data Subject shall be entitled to all available judicial remedies, including but not limited to compensation for damages (both material and non-material) as a result of any unlawful processing of the Personal Data and nothing in this Agreement shall limit the rights of the Data Subject to avail of such remedies.

8.9 Each of the Parties shall notify the other of them, on a timely basis, of the outcome of any proceedings concerning the notifying Party, including

	where a complaint of any Data Subject is dismissed or not resolved. Where the Parties do not succeed in resolving a dispute with a Data Subject amicably, then the transferring Party is entitled to suspend or terminate the transfer of Personal Data under the Agreement until the matter has in the view of the transferring Party been satisfactorily addressed by the transferee Party. Where such suspension or termination occurs, then the receiving Party is required to return or delete the Personal Data concerned at the request of the transferring Party and the transferring Party is required to notify the suspension or termination to the relevant Supervisory Authority.
9.	**Security and Storage of Personal Data** 9.1 The Parties undertake to have in place appropriate technical and organisational security measures to: (a) prevent: (i) unauthorised or unlawful processing of the Shared Personal Data; and (ii) the accidental loss or destruction of, or damage to the Shared Personal Data (b) ensure a level of security appropriate to: (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and (ii) the nature of the Shared Personal Data to be protected. 9.2 To ensure confidentiality, all relevant staff involved in discussions across the organisations will adopt steps that can reduce the risks to Personal Data. 9.3 The sharing of recorded / written information will be by secure means at all times. If transferred electronically, this will be through encrypted e-mail transport or encrypted, authenticated file sharing application and additionally the document payload shall also be encrypted and password protected. 9.4 Emails will only be sent to healthprotectionhpsc@hpsc.ie or NIContacttracing@hscni.net recognised domains which have been added to a white list. Only authorised staff that would normally have access to this data as part of their duties will transfer / receive this information. Validation of the transfer process by confirming receipt of transmissions is necessary to further ensure only legitimate communications are accepted. 9.5 For the PHA where the confirmed case provides details of one or more contacts who live in the Republic of Ireland (RoI), the details of the contacts will be sent to the HPSC. The information will be sent via encrypted email to healthprotectionhpsc@hpsc.ie. Any urgent issues that require public health actions out of hours are shared by phone with the doctor on call for

HPSC (as per Data Flow section 5 Appendix 2). The HPSC disseminate the information to the relevant Department of Public Health in RoI. In the event that a large number of contacts have been identified a document containing the information will be sent via an encrypted email.

9.6 For the HSE where the confirmed case provides details of one or more contacts who live in Northern Ireland, the details of the contacts will be sent to the PHA. The information will be encrypted, password protected and encryption emailed to nicontacttracing@hscni.net. Urgent information will be communicated by phone. A record of information shared by or video call phone shall be kept by both Parties. Other sharing should be auditable through file transfer records.

9.7 Measures will be in place to ensure that Personal Data, both manual and electronic, is stored and transported by secure means at all times and only authorised staff will have access to this Personal Data as part of their duties.

9.8 It is the responsibility of each Party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with appropriate technical and organisational security measures and Data Protection Legislation.

9.9 For the HSE, Personal Data is protected by the HSE in accordance with the HSE's Privacy Statement which can be accessed via https://www.hse.ie/eng/privacy-statement/. The HSE's COVID-19 specific information notice can be accessed via https://www.hse.ie/eng/gdpr/data-protection-covid-19/.

9.10 HSE maintains strict information security and data protection policies and procedures across all areas of the HSE. HPSC maintain and Information Security Management System (ISMS) that is certified to ISO27001. The HPSC ISMS also manages data protection obligations of staff, including comprehensive ongoing training.

For the PHA the Contact Tracing Service Privacy Notice can be accessed at https://www.publichealth.hscni.net/covid-19-coronavirus/testing-and-tracing-covid-19/privacy-information

The security of the PHA Contact Tracing Service and Information System is set out in the PHA Contact Tracing Service DPIA.

9.11 PHA and HSE – Security in consideration of the Parties sharing Data with each other, each Party agrees that it shall:

Maintain the security and confidentiality of all Personal Data and Special

	Categories of Personal Data shared under this Agreement; Process all Personal Data and/or Special Categories of Personal Data shared under this Agreement in accordance with Data Protection Legislation; Ensure that access to any Personal Data and/or Special Categories of Personal Data which they receive from the other Party is limited to those of their employees and contractors who need to have access to it, and that they are informed of the confidential nature of the Personal Data and Special Categories of Personal Data, are under an obligation to keep such Personal Data and Special Categories of Personal Data confidential, and comply with the obligations set out in this Agreement; Ensure all their relevant employees and contractors with access to the Personal Data and/or Special Categories of Personal Data have been provided with appropriate data protection and IT security training; Implement Appropriate Technical and Organisational Measures (TOM's) within their own organisation to protect against the unauthorised or unlawful processing and the accidental loss, destruction, damage, alteration and disclosure of any Personal Data and/or Special Categories of Personal Data which is shared under this Agreement. As a minimum, the following TOM's shall be implemented by each of the Parties: Strong and robust access controls are in place to manage and protect access to Personal Data and Special Categories of Personal Data; Access to Personal Data and Special Categories of Personal Data stored electronically is controlled by strong unique passwords; All mobile computer devices which are used to Process and/or store Personal Data and Special Categories of Personal Data have strong encryption facilities available which allow for the encryption of the mobile computer device and/or the encryption of the Personal Data Special Categories of Personal Data at a file or folder level; All computer devices which are used to Process or store Personal Data Special Categories of Personal Data have real-time protection anti-malware software installed which is updated on a regular basis; All Personal Data and Special Categories of Personal Data which is Processed or stored off-site or within a cloud computing solution by a third party on behalf of a Party is encrypted at rest using strong encryption protocols; All Personal Data and/or Special Categories of Personal Data transmitted via electronic means outside their organisation is sent via secure channels (for example, VPN, Secure FTP, TLS) or encrypted email using strong

	encryption protocols; All Personal Data and/or Special Categories of Personal Data is backed up on a regular basis and backup copies of the data are tested on a frequent basis to ensure the data can be restored in the event of a hardware or software crash or a cyber-security incident; Appropriate processes are in place which allows each Party to regularly test, assess and evaluate the effectiveness of the TOMs they have implemented within their organisation The level of security to be applied by the Parties will take into consideration the risks, the state of the art and the related costs. Each Party have documented IT and information security policies which define how the Party's employees, contractors and third parties are to manage, process and secure the Party's data.
10.	**Retention and disposal** 10.1 All Personal Data held is for the specific purpose stated in section 3 of this Agreement. Personal Data must not be held for any longer than is necessary to carry out the task(s) agreed in Section 3. 10.2 Each of the Parties must retain and dispose of information in accordance with their organisational retention and disposal policy. Personal Data shared under this Agreement which has reached the end of its legal retention period and is no longer required shall be disposed of securely in accordance with each organisation's disposal policies. 10.3 For the PHA, the data will only be held for as long as necessary in line with the PHA Retention and Disposal Schedule (Good Management, Good Records) and specific guidance issued by the Department of Health in Northern Ireland. Good Management, Good Records (GMGR) is the DoH retention and disposal schedule that all HSC organisations in NI are required to comply with, and can be found at: https://www.health-ni.gov.uk/topics/good-management-good-records 10.4 For the HSE no Party shall retain Personal Data or Special Categories of Personal Data shared under this Agreement for longer than is necessary and such records shall be held in line with the HSE's record retention policy available on its website, as follows:- https://www.hse.ie/eng/services/list/3/acutehospitals/hospitals/ulh/staff/resources/pppgs/rm/recret.html
11.	**Security incidents or Data Breaches** 11.1 Security of information will be managed in line with each organisation's protocols and standards to eliminate any Data Breaches. Any security breach incident involving Personal Data should be reported at the earliest

	opportunity through the organisations incident reporting system and to the relevant Information Governance Lead, and investigated in line with the organisation's Data Breach policy. Where appropriate, the Parties will inform the point of contact in the other organisation immediately. Each Party will also follow the relevant requirements to notify the DPC (RoI) or ICO (NI) in accordance with Data Protection Legislation. 11.2 Examples of serious Data Breaches may include: • accidental loss or damage to the Personal Data; • damage or loss of Personal Data by means of malicious software/hacking; • deliberate or knowingly disclosure of Personal Data to a person not entitled to receive the Personal Data; • emailing classified/sensitive information containing Personal Data to personal email accounts; • leaving classified/sensitive papers containing Personal Data in an unsecure or publicly accessible area; using social networking sites to publish information containing Personal Data which may bring either Party's organisations into disrepute. 11.3 In the event that either Party becomes aware of a Data Breach, that Party shall fulfil its obligation to notify the DPC or the ICO as required and/or Data Subjects of the Data Breach in accordance with Articles 33 and 34 of the GDPR. Both Parties are responsible for notifying regulator that is applicable to their jurisdiction. 11.4 The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Data Breach in an expeditious and compliant manner. The designated points of contact will discuss the next steps relating to the incident, taking specialist advice where appropriate. Such steps may include (but may not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the Personal Data, and assessing whether the DPC, the ICO and/or the Data Subjects will be notified. The steps may vary in each case, depending on the sensitivity of the Personal Data and the nature of the loss or unauthorised disclosure.
12.	**Review/Termination of Agreement** 12.1 If any significant change takes place which means this Agreement becomes an unreliable reference point, this Agreement will be updated as needed and a new version circulated to replace it. Either signatory to this Agreement can request an extraordinary review at any time. 12.2 This Agreement will be reviewed six months after the date stated at the beginning of it (or earlier if considered necessary by either Party) and

	three months thereafter. The responsible officer (service lead) in each organisation will carry out the reviews. 12.3 Either Party may terminate this Agreement by providing the other Party with thirty (30) calendar day's written notice of their intention to terminate the Agreement.
13.	**Declaration** 13.1 The Parties will comply with Data Protection Legislation, and any associated guidelines issued by relevant authorities. **The Parties agree that:** • The information shared is for a specified, explicit and legitimate purpose • It is adequate, relevant and limited to what is necessary in relation to the purposes for which it is transmitted and further Processed • It will be processed fairly and lawfully and used only for the stated purpose • It will be processed and stored in a manner that ensures appropriate security • It will be held no longer than is necessary for the stated purpose • It will be kept accurate and up to date having regard to the purposes for which it is Processed and if one of the Parties becomes aware that any Personal Data which has been transmitted or is being processed is out of date, it shall notify the other Party without delay and in these circumstances each Party Processing the Personal Data shall take every reasonable step to rectify or erase the relevant Personal Data. • It will be disposed of fully and in such a way that it is not possible to reconstitute it • All measures will be taken to ensure identifiable data is not disclosed to third parties without appropriate prior authority of each of the Parties. • Where appropriate, the Parties will be informed of the identifiable data being deleted / destroyed • Any loss, theft or corruption of the shared Personal Data will be immediately reported to the authorised officer of the owning organisation and the other Party will assist fully in any investigation. Any serious breaches, data loss, theft or corruption will be reported to the relevant authority within 72 hours of the Data Breach first being discovered.

14.	**Indemnity** 14.1 The Parties agree to indemnify each other, against all damages, losses, liabilities, cost, fines and/or penalties, expenses, compensation and associated costs arising out of or in connection with any act, omission, default or negligence of a Party relating to Processing of Personal Data and Special Categories of Personal shared under this Agreement. 14.2 This Clause 14 is intended to apply to the allocation of liability for losses relating to Data Protection Legislation as between the Parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Legislation to the contrary, except (i) to the extent not permitted by applicable law. (including Data Protection Legislation); and (ii) that it does not affect the liability of any Party to any Data Subject. 14.3 The provisions of this section 14 shall survive the termination or expiry of this Data Sharing Agreement.
15.	**Supervision Mechanisms** 15.1 Each of the Parties shall ensure that they have sufficiently robust internal supervision mechanisms in place in their respective organisations to adequately protect Data Subjects and ensure compliance with the Agreement. Each Party will conduct periodic internal checks of the procedures in place and the effective application of the safeguards provided for in this Agreement. 15.2 Each of the Parties shall also be entitled to request that the other Party carry out such a review and the Party conducting the review will be required to communicate the results of the review to the other Party. 15.3 Each of the Parties will be required (i) to respond to inquiries from the other Party concerning the effective implementation of the safeguards in the Agreement; and (ii) to inform the other Party without delay if they are unable to effectively implement the safeguards in the Agreement for any reason. The transferring Party is entitled in these circumstances, to suspend or terminate the transfer of Personal Data under the Agreement until such time as the receiving Party informs the transferring Party that it is again able to act consistent with the safeguards. Where such suspension or termination occurs, then the receiving Party is required to return or delete the Personal Data concerned at the request of the transferring Party and the transferring Party is required to notify the suspension or termination to the relevant Supervisory Authority. 15.4 The independent redress and supervision mechanism available to Data Subjects under this Agreement will be satisfied by independent, effective and impartial external oversight from, in the case of the HSE, the DPC and in the case of the PHA, the ICO.

16.	**Governing Law and Jurisdiction** 16.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with: i) For acts or omissions of the PHA by the law of Northern Ireland; ii) For acts or omissions of the HSE by the law of Ireland. 16.2 Proceedings instituted against PHA by the HSE shall be brought in the courts of Northern Ireland and any such proceedings against HSE by PHA shall be brought in the courts of Ireland. This clause is without prejudice to the rights of redress or to an effective judicial remedy of third parties under Data Protection Legislation.
17.	**Disputes** 17.1 Where any dispute or difference arises between Parties in relation to any alleged breach of this Agreement, the parties undertake that they shall forthwith meet to discuss the subject matter of the dispute and shall each use all reasonable endeavours in good faith to resolve the dispute amicably by agreement. 17.2 In the event that the parties are unable to resolve the dispute within twenty – eight (28) days from the date of the meeting referred to in Clause 17.2, then the parties shall by notice in writing refer the matter to mediation by a person agreed between the Parties.
18.	**Counterparts** 18.1 This Agreement may be executed in several counterparts or duplicates, each of which counterparts shall be deemed an original document but all of which taken together shall constitute one single agreement between the Parties. Each Party agrees that it and each other Party may execute this Agreement by way of e-signature, and agrees that execution in such manner will be valid and binding on each of the parties hereto. No Party executing this Agreement by way of e-signature shall seek to avoid its responsibilities under this Agreement based on the fact that it signed this Agreement using an e-signature as opposed to a hand-written signature on paper. Transmission of an executed counterpart of this Agreement (or of the executed signature page of a counterpart of this Agreement) by email (in PDF, JPEG or other agreed format) or any electronic document signing platform (including, but not limited to DocuSign) shall take effect as delivery of an executed counterpart of this Agreement.
19.	**Execution Requirements** 19.1 This document has been executed as a deed and is delivered and

	takes effect on the date stated at the beginning of it. 19.2 Each of the Parties warrant that their respective nominated signatories to this Agreement have full power and authority to execute this Agreement for and on behalf of the relevant Party in accordance and compliance with their internal requirements as to execution of documents and that this Agreement constitutes a valid, legally binding and enforceable obligation on each of the Parties in accordance with its terms.

Appendix 1a:- Standing Operating Procedure (SOP)

SOP for COVID19 information sharing between Republic of Ireland (RoI) and Northern Ireland (NI)

1. RoI reporting cases/contacts to NI:

- All information is to compiled according to minimal data set as laid out in Data Sharing Agreement (DSA) in agreed excel template (case or close contact excel file as appropriate)
- HPSC send completed password protected file to: nicontacttracing@hscni.net
- All @hpsc.ie and @hse.ie emails have been added to the white list to allow communication directly with NI
- **Close contact information that is sent to HPSC after 9pm is communicated the following morning to the PHA in NI to** nicontacttracing@hscni.net. This is at the discretion of the Specialist on call in RoI.

Contact number for the PHA (NI):

- From 8am to 9pm, 7 days a week- 028 95 360405 (Contact tracing lead only available at this number until 5pm).
- For out of hours (5pm – 8am) **0044 2890 404045*. First on call HP Reg via Ambulance Control**

***Please note these numbers are not for wider distribution and should only be used when urgent issues need to be discussed with a Health Protection specialist. There is no requirement to contact for general sharing of contact/case information; information of this nature should be communicated by the above steps to** nicontacttracing@hscni.net

2. NI Reporting Cases/contacts to ROI

- All information is to compiled according to minimal data set as laid out in Data Sharing Agreement (DSA) in agreed excel template (case or close contact excel file as appropriate)
- The Public Health Agency NI will send completed password protected file to: healthprotectionhpsc@hpsc.ie.
- Emails are screened by the on-call support team in HPSC.
- Details regarding close contacts are sent to CTCs and details regarding cases are sent to the relevant Department of Public Health in RoI.

Contact number for the HPSC (RoI) as follows:

- From 9am to 5pm Monday to Friday please consult the **Health Protection specialist rota (this is sent out every month – specialist varies daily).**
- **Out of hours from 5pm Monday to Friday and all day Saturday and Sunday please contact** the Health Protection specialist on call. Rota is distributed to NI monthly.

3. Process of loading RoI data onto Microsoft Dynamics (For NI only)

- The contact/case data will be received via password protected excel file into the nicontacttracing@hscni.net email address.

- This is accessed by the Clinical Lead in the CTC. The information is risk assessed and appropriate action is taken. If action is needed, the CTC lead will forward the email with the contact information to the Administrative staff. They will load the data onto Microsoft Dynamics.

    - Cases – a text will be sent out to each case loaded onto Microsoft Dynamics inviting the case to self-trace. If the case does not act on this then a contact tracer will pick up the case and carry out contact tracing by phone. Contacts are identified by the contact tracer and loaded directly onto Microsoft Dynamics.

    - Contacts – an automatic text will be sent out alerting the individual to their personal mobile that they have been identified as a contact.

4. Cross Border Communication:

The following is a list of cross border meetings that occur at frequent intervals.

- Weekly teleconference-Data Sharing Agreement, RoI Border County, HPSC and NI representation.
- Daily RoI Border County and NI phone call.
- Fortnightly track and Trace teleconference-Chaired by Department of Health RoI. HPSC, HSE DPH and CTC and NI PHA and CTC representations
- Weekly Health Protection-Cross border Health Protection committee chaired by HP leads in RoI and NI.

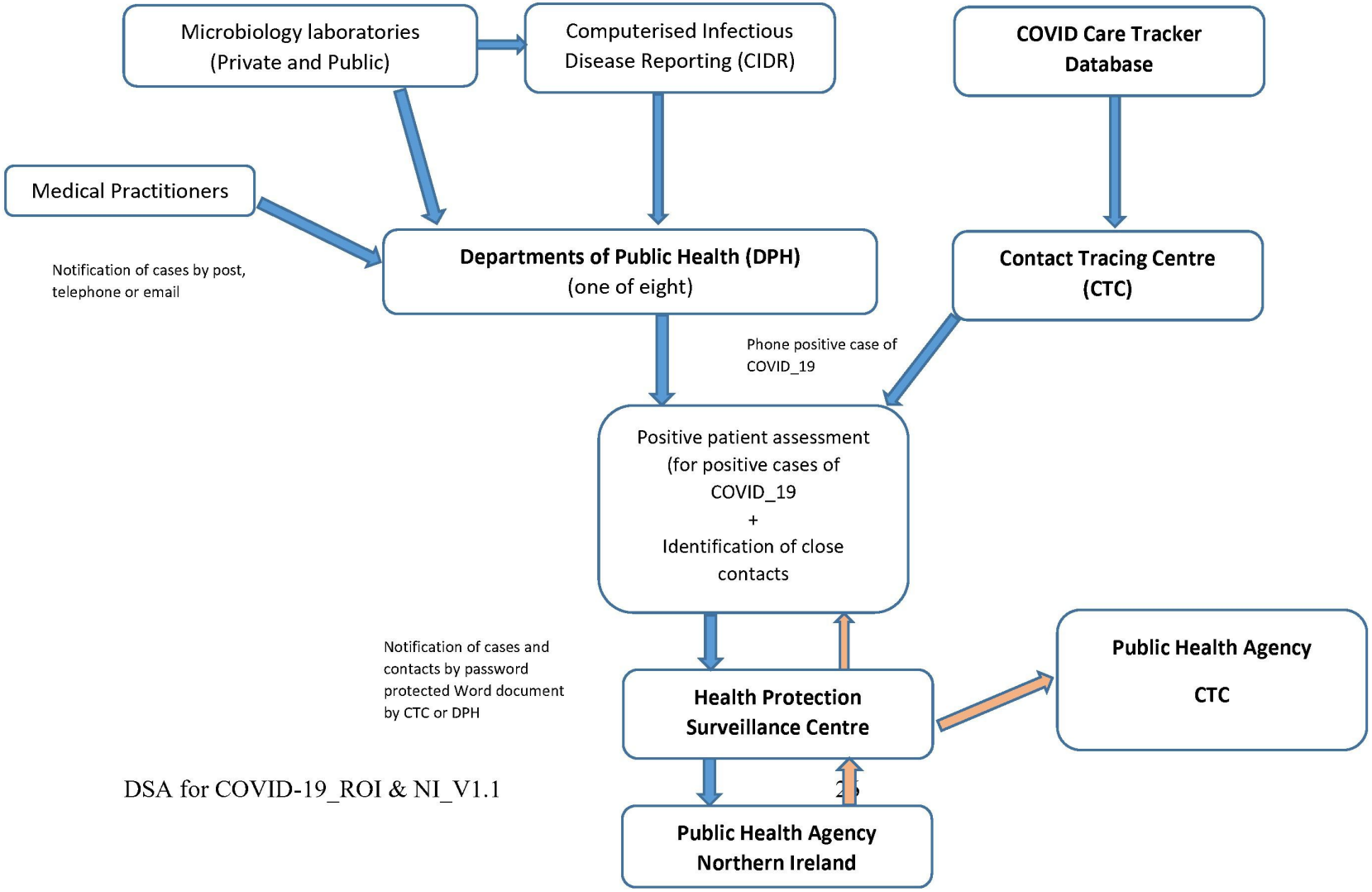
This will allow for;

- better management of cross border outbreaks, or raise issues/areas of concern
- Exchange of "knowledge behind the data" and ensure we have a regular channel of open communication between RoI and NI.
- Operational decisions around establishing Incident Management Teams in cross border clusters/outbreaks.

Appendix 1b:- Data Flow Chart

COVID-19 notifications

Data flows for positive cases of COVID-19 and close contacts from RoI to NI → From NI to RoI →



Appendix 2

GLOSSARY

Agreement – means this Data Sharing Agreement

Anonymised data – information from which no individual can be identified.

Appropriate Safeguards means the measures set out in Article 46 of GDPR.

Appropriate Technical and Organisational Measures or **TOMs** - the appropriate technical and organisational measures referred to in Data Protection Legislation (including, as appropriate, the measures referred to in Article 32(1) of GDPR);

Contact - Someone who was within 6 feet of an infected person for a cumulative total of 15 minutes or more over a 24-hour period.

Contact Tracing - is an established and recognised methodology for controlling and reducing the spread of communicable infectious diseases such as COVID 19, that is used nationally and internationally to contact trace close contacts of persons who have tested positive for such diseases.

CTC – Contact Tracing Centre

Data Breach - means any Personal Data breach as described in GDPR in respect of the Personal Data and Personal Data Breaches shall be interpreted accordingly;

Data controller – a person or organisation who (either alone or jointly or in common with other persons or organisations) determines the purposes for which and the manner in which any personal information is to be processed. (refer to GDPR Article 24 for further details on the responsibility of the Controller)

Data processor – any person or organisation (other than an employee of the data controller) who processes information on behalf of the data controller. (refer to GDPR Article 28 for further details on the responsibility of a Processor)

Data Protection Act 2018 (DPA 2018) UK – the main UK legislation governing the handling and protection of information relating to living people.

Data Protection Act 2018 (DPA 2018) RoI – the main ROI legislation governing the handling and protection of information relating to living people.

Data Protection Officer – Named, appointed individual within a department responsible for providing assurance to departmental board regarding DPA 2018/ GDPR compliance.

Data Protection Impact Assessment (DPIA) – a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

Data Protection Legislation – means all applicable data protection and privacy legislation in force including GDPR, and the Data Protection Act 2018 (DPA 2018) UK and the Data Protection Act 2018 (DPA 2018) ROI as such legislation shall be supplemented, amended, revised or replaced from time to time and all guidance and codes of practice issued by the DPC, the ICO and the EDPB from time to time;.

Data protection principles – six rules which all organisations processing personal data must conform to under Article 5 of GDPR (plus accountability principle)

Data Subject – an individual who is the subject of the personal data.

Data sharing – the disclosure of data from one or more organisations to a third-party organisation or organisations, or the sharing of data between different parts of an organisation. It can take the form of systemic, routine data sharing where the same information is shared between the same organisations for an established purpose, or one-off decisions to share data for any of a range of purpose.

Dispute – any dispute or difference that arises between the Parties in relation to any alleged breach of this Agreement

DPC - means the Data Protection Commission

EEA - European Economic Area means those states that are contracting parties to the Agreement on the European Economic Area from time to time and includes the United Kingdom until it ceases to be subject to the transition or implementation arrangements provided for by Part 4 of the Withdrawal Agreement between the United Kingdom and the European Union.

EDPB – means the European Data Protection Board.

General Data Protection Regulation (GDPR) – means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing the Directive 95/46/EC (General Data Protection Regulation), and any amendments made thereto;

HPSC – means the Health Protection Surveillance Centre of the HSE.

ICO – Information Commissioner's Office

Index Case – the first documented case of an infectious disease or genetically transmitted condition or mutation in a population, region, or family

Personal Data – information which relates to a living individual who can be identified from that information and other information in the possession of the data controller. It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing – is any activity involving use of Personal Data as set out in GDPR and Process and Processed shall be interpreted accordingly. This includes obtaining, recording or holding the data or doing any work to it such as organising, adapting, changing, erasing or destroying it.

Restricted Transfers any transfer of Personal Data to countries outside of the EEA which are not subject to an adequacy decision by the European Commission, where such transfer would be prohibited by Data Protection Legislation.

Shared Personal Data means the Personal Data shared for the agreed purposes set out in Section 3 of the Agreement.

Subject Access Request (SAR)– a request (can be written or verbal) from an individual for information that is held about them.

Special categories of personal data or Special Category Data – personal information about an individual's race or ethnic origin; political opinions; religious or other similar beliefs; trade union membership; health; sexuality; biometric data and genetic data. Special categories of personal data can only be processed under strict conditions.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Standard Contractual Clauses the contractual clauses dealing with the transfer of Personal Data outside the EEA, which have been approved by (i) the European Commission under Data Protection Legislation, or (ii) by the DPC or the ICO or an equivalent competent authority under Data Protection Legislation.

HSC Public Health Agency

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Appendix 3 - Principles Governing Personal Data Sharing[1]

Code of Practice Principles	GDPR Principles	Caldicott Principles[2]
The Code of Practice is principally concerned with identifiable service user information. The nature of the obligation to protect confidentiality can be expressed in terms of three core principles: • individuals have a fundamental right to the confidentiality and privacy of information related to their health and social care; • individuals have a right to control access to and disclosure of their own health and social care information by giving, withholding or withdrawing consent; • when considering whether to disclose confidential information, health and social care staff should have regard to whether the disclosure is necessary, proportionate and accompanied by any undue risks. Particular care is needed on the part of health and social care staff to ensure that the right to privacy of vulnerable people – specifically adults with	**1.** processed lawfully, fairly and in a transparent manner **2.** Purpose limitation - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **3.** Data minimisation - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **4.** Data Quality - accurate and, where necessary, kept up to date **5.** Storage Limitation - kept for no longer than is necessary. **6.** Integrity and Confidentiality - processed in a manner that ensures appropriate security of the personal data **7.** Overarching Accountability principle – take responsibility for what you do with personal data and how you comply with the other principles, having appropriate	**1.** Justify the purpose(s) for using confidential information. **2.** Only use it when absolutely necessary. **3.** Use the minimum that is required. **4.** Access should be on a strict need-to-know basis. **5.** Everyone must understand his or her responsibilities. **6.** Understand and comply with the law. **7.** The duty to share information can be as important as the duty to protect patient confidentiality

[1] These principles must be followed by health and social care organisations when considering use and disclosure of service user information.
[2] PDG Principles are adopted from the Caldicott Principles (revised September 2013) established in England and Wales.

incapacity and children – is respected and that the duty of confidentiality owed to them is fulfilled. https://www.health-ni.gov.uk/publications/code-practice-protecting-confidentialityservice-user-information	measures and records in place to be able to demonstrate your compliance. Principles relating to individuals' rights and overseas transfers of personal data are specifically addressed in separate GDPR articles.	

Executed as deed by Public Health Agency acting by Dr. Stephen Bergin a director, in the presence of:

Personal Data

Dr **NR**, Assistant Director of Public Health (Health Protection), PHA, 12-22 Linenhall Street, Belfast BT2 8BS

Personal Data

Dr Stephen Bergin, Director of Public Health (Interim), PHA, 12-22 Linenhall Street, Belfast BT2 8BS

Executed as deed by the HSE acting by Dr. Lorraine Doherty, a director, in the presence of:

Personal Data

Dr. NR Interim Director of HPSC, 25-27, Middle Gardiner Street, Dublin 1.

Personal Data

Dr Lorraine Doherty, National Clinical Director for Health Protection, HPSC, 25-27, Middle Gardiner Street, Dublin 1.