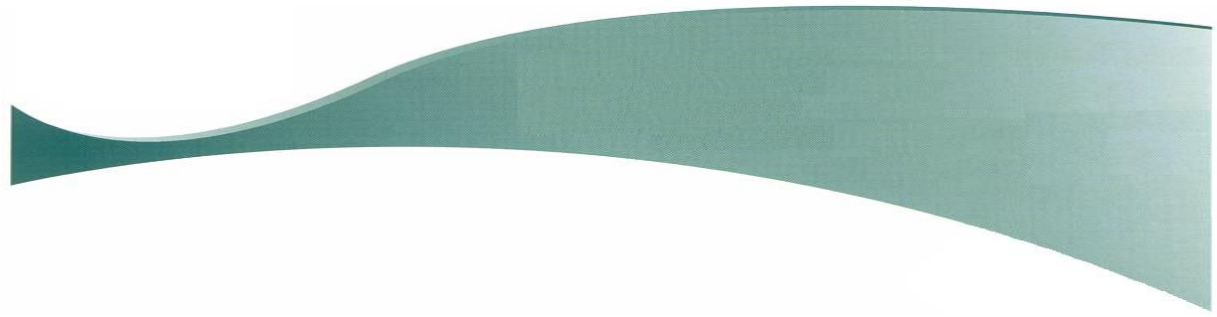
Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Service Provider
Data Processing Agreement



Version 2.0

THIS AGREEMENT is dated …… and made between:

(1) **The Health Service Executive**, a body corporate with perpetual succession established by the Health Act 2004 (the **HSE**), and

(2) ……..
(the **Service Provider's** name (Block Capitals))

……
(the **Service Provider's** registration number **(**Block Capitals**)**)

……
(the **Service Provider's** registered office **(**Block Capitals**)**)

RECITALS

A. The Service Provider provides one or more services (the **Services**) to the HSE. The HSE and the Service Provider have entered into one or more written service agreements pursuant to the provision of these Services (collectively, the **Contract(s)**). This Agreement is an addendum to any and all Contracts between the HSE and the Service Provider.

B. Unless agreed otherwise by the HSE and the Service Provider, where any of the Services provided under Contract to the HSE, involve the Service Provider processing Personal Data on behalf of the HSE, the HSE shall be considered the Data Controller or Joint Data Controller of the HSE Personal Data and the Service Provider shall be considered the Data Processor.

C. The HSE shall comply at all times with its obligations as a Data Controller or Joint Data Controller as set out in the Data Protection Legislation.

D. Appendix 1 contains a description of the subject matter, duration of the Processing, nature and purpose of Processing, as well as the type of Personal Data and categories of Data Subjects' Personal Data Processed by the Service Provider under this Agreement.

E. This Agreement will cover the Service Providers Processing of any and all HSE Personal Data under any and all Contracts between the HSE and the Service Provider.

NOW IT IS HEREBY AGREED by and between the parties hereto as follows:

1 Definitions:

In this Agreement, unless the context otherwise requires:

Agreement shall mean the HSE Service Provider Data Processing Agreement (SPDP);

Data Controller or Controller has the meaning given to that term in Article 4 of the GDPR;

Data Processor or Processor has the meaning given to that term in Article 4 of the GDPR;

Data Protection Commission means the Irish Data Protection Commission which is the Irish data protection supervisory authority;

Data Protection Legislation means all applicable laws and regulations relating to the processing of Personal Data and privacy including the Data Protection Act 2018, the General Data Protection Regulation 2016/679 (the "GDPR") and the European Communities (Electronic Communications, Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336/2011) and any statutory instrument, order, rule or regulation made thereunder, as from time to time amended, extended, re-enacted or consolidated;

Data Subject has the meaning given to that term in Article 4(1) of the GDPR;

Delete, Deleted, Deletion and like words, shall mean the permanent removal of data and all traces of the data, by means of the physical destruction of the data, or the physical destruction of the medium used to store the data, or the overwriting of the data, in accordance with internationally accepted data erasure standards using data sanitation software;

GDPR means the EU General Data Protection Regulation, Regulation (EU) 2016/679, the effective date of which is 25th May 2018;

HSE Personal Data shall mean the Personal Data and Special Categories of Personal Data Processed by the Service Provider on behalf of the HSE as more specifically detailed in Appendix 1;

Personal Data has the meaning given to that term in Article 4 of the GDPR;

Personal Data Breach has the meaning given to that term in Article 4 of the GDPR;

Processing, Process and like words**,** have the meaning given to those terms in Article 4 of the GDPR;

Pseudonymisation, Pseudonymised and like words**,** have the meaning given to those terms in Article 4 of the GDPR;

Special Categories of Personal Data has the meaning given to that term in Article 9(1) of the GDPR;

Sub-Processors shall mean any person or legal entity which is not party to any Contract(s) between the HSE and the Service Provider and this Agreement, and which is engaged by the Service Provider to perform any or all of its obligations in relation to the Processing of HSE Personal Data, including for the avoidance of doubt, a Service Provider group company including subsidiaries and affiliates;

2 Obligations of the Service Provider

2.1 To the extent that the Service Provider Processes HSE Personal Data as a Data Processor on behalf of the HSE, the Service Provider shall:

2.1.1 Comply at all times with their obligations as a Data Processor as set out in the Data Protection Legislation and this Agreement, and not undertake any actions or permit any actions to be undertaken on their behalf which may cause the HSE to be in breach of the Data Protection Legislation;

2.1.2 Manage and Process any HSE Personal Data they acquire from the HSE solely in accordance with the documented instructions of the HSE as set out in this Agreement, including with regard to transfers of HSE Personal Data to a third country or an international organisation, unless required to do so by European Union or Irish Law to which the Service Provider is subject; in such a case, the Service Provider shall inform the HSE in writing of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

2.1.3 Notify the HSE prior to carrying out any instruction from the HSE if, in the Service Providers opinion, such instruction is likely to result in Processing that is in breach of the Data Protection Legislation;

2.1.4 Only Process and use HSE Personal Data for the purposes of providing any contracted Services to the HSE and, not otherwise modify, amend or alter the contents of HSE Personal Data unless specifically authorised to do so in writing by the HSE;

2.1.5 Take all reasonable measures to ensure the reliability of any of the Service Providers employees and contractors who have access to HSE Personal Data;

2.1.6 Ensure that access to HSE Personal Data is limited to those of the Service Provider's employees and contractors who need to have access to it, and that they are informed of the confidential nature of the HSE Personal Data, are under an obligation to keep such HSE Personal Data confidential, and comply with the obligations set out in this Agreement;

2.1.7 Ensure that all the relevant Service Provider employees and contractors with access to HSE Personal Data have been provided with and have undergone appropriate Data Protection and IT security training;

2.1.8 Ensure they have appropriate procedures in place which prevent the Service Provider's employees and contractors from downloading HSE Personal Data from the Service Provider's IT devices and Servers and storing this HSE Personal Data on the employees' or contractors' personal IT devices (i.e. where the IT device is the personal property of the employee or contractor and not the Service Provider);

2.1.9 Ensure they have appropriate processes implemented and documented which will allow the Service Provider to promptly and effectively detect, contain, analyse,

respond and recover from any suspected or actual information security and cyber security incidents within their organisation, and where necessary to promptly notify the HSE of any such incidents involving HSE Personal Data;

2.1.10 Ensure all printouts taken by the Service Providers employees and contractors containing HSE Personal Data are managed and stored appropriately and, disposed of securely when they are no longer required;

2.1.11 Not disclose or permit the disclosure of any the HSE Personal Data to any third party unless specifically authorised to do so in writing by the HSE. In the event that the Service Provider is legally required to disclose any HSE Personal Data to a third party, the Service Provider undertakes to notify the HSE of such requirement prior to any disclosure and, unless prohibited by law, to supply the HSE with copies of all communications between the Service Provider and any third party to which such disclosure is made. At the request of the HSE, the Service Provider shall co-operate with the HSE in bringing any legal or other proceedings to challenge the validity of the requirement to disclose the HSE Personal Data;

2.1.12 At no additional cost to the HSE, and while taking into account the nature of Processing, assist the HSE by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the HSE's obligations to respond to requests from Data Subjects, exercising their rights laid down in Chapter III of the GDPR (including their right of access, rectification of and erasure of their Personal Data). Upon a request from the HSE for such assistance, the Service Provider shall comply with the request in a timely manner, so as to allow the HSE comply with its legal obligations concerning the timescales for responding to such requests from Data Subjects, as laid down in Article 12 of the GDPR;

2.1.13 At no additional cost to the HSE, and while taking into account the nature of Processing and the information available to the Service Provider, assist the HSE in ensuring compliance with the obligations pursuant to Articles 32, 33, 34 and 36 of the GDPR (including the security of HSE Personal Data, Personal Data Breach notifications, and prior consultations) including without limitation the preparation or provision of supporting documentation to be submitted to the Data Protection Commission;

2.1.14 Assist the HSE in relation to any assessment, enquiry, notice or investigation received by the HSE from the Data Protection Commission which may include (as appropriate) the provision of data requested by the HSE within the timescales reasonably specified by the HSE in each case.

3 Data Protection Impact Assessments

3.1 At no additional cost to the HSE, while taking into account the nature of Processing and the information available to the Service Provider, the Service Provider shall provide all

reasonable assistance to the HSE in the preparation of any assessment by the HSE of the impact of the envisaged Processing on the protection of HSE Personal Data ("Data Protection Impact Assessment") prior to commencing any Processing. Such assistance may, at the discretion of the HSE, include assistance regarding the preparation of the following:

3.1.1 A systematic description of the envisaged Processing operations and the purpose of the Processing;

3.1.2 An assessment of the necessity and proportionality of the Processing operations in relation to the Services;

3.1.3 An assessment of the risks to the rights and freedoms of Data Subjects; and

3.1.4 The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of HSE Personal Data.

4 Technical & Operational Measures

4.1 The Service Provider shall implement appropriate technical and organizational measures to protect against the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to HSE Personal Data processed by the Service Provider;

4.2 Where the Service Provider uses their own ICT resources (i.e. ICT resources which are owned or controlled by the Service Provider) to Process or store HSE Personal Data, the Service Provider must implement the minimum technical and organizational measures set out in Appendix 3 of this Agreement to protect the HSE Personal Data;

4.3 At the written request of the HSE, the Service Provider shall provide the HSE within 7 calendar days, with a written description of the technical and organisational measures implemented by the Service Provider and (as applicable) their Sub-Processors to protect HSE Personal Data they Process.

5 Appointment of Sub-Processors

5.1 The Service Provider shall not engage any Sub-Processors to Process HSE Personal Data other than with the prior written consent of the HSE. For the avoidance of doubt, HSE written consent shall be deemed given for the authorised Sub-Processors listed in Appendix 2 of this Agreement;

5.2 The Service Provider shall inform the HSE in writing of any intended changes concerning the addition or replacement of other Sub-Processors who will Process HSE Personal Data, thereby giving the HSE the opportunity to object to such changes where it considers that such Sub-Processors do not provide sufficient guarantees under the Data Protection Legislation. In the event that the HSE objects to the addition or replacement of Sub-Processors, the Service Provider shall use reasonable endeavour's to address the HSE's concerns;

5.3 Where the Service Provider engages a Sub-Processor to Process HSE Personal Data, the Service Provider shall impose obligations on the Sub-Processor, by way of a separate contract / agreement between the Service Provider and the Sub-Processor, which includes terms that are the same as, or equivalent to those terms set out in this Agreement. The Service Provider shall ensure that Sub-Processors engaged by them to Process HSE Personal Data, cease Processing HSE Personal Data upon the earlier termination of this Agreement or the termination of the Service Provider's contract / agreement with the Sub-Processor. The Service Provider shall remain fully liable to the HSE for any failure by a Sub-Processor to fulfil its obligations in relation to the Processing of any HSE Personal Data.

6 International Data Transfers

6.1 The Service Provider shall not process and/or transfer any HSE Personal Data in or to any country outside the European Economic Area (EEA) without the prior written consent of the HSE;

6.2 Where the HSE has consented to the Service Provider processing and/or transferring HSE Personal Data in or to a country outside the EEA, the Service Provider may only process and/or transfer HSE Personal Data in or to:

6.2.1 A country outside the EEA in respect of which an adequacy decision made by the European Commission under Article 45(3) of the GDPR is in force;

6.2.2 A country outside the EEA subject to the execution of standard data protection clauses adopted by the EU Commission in accordance with the examination procedure referred to Article 93(2) of the GDPR, as provided for in Article 46(2)(c) and Article 46(2)(d) of the GDPR (the 'Standard Contractual Clauses') as between:

(a) the HSE and the Service Provider (where the Service Provider is receiving the HSE Personal Data (i.e. it is the data importer)); and/or as applicable

(b) the Service Provider and a Sub-Processor approved in accordance with Clause 5, where the Service Provider is transferring the HSE Personal Data (i.e. it is the data exporter) and the Sub-Processor is receiving the HSE Personal Data (i.e. it is the data importer).

6.2.3 A country outside the EEA but where the transferee (i.e. the data importer) of the HSE Personal Data is a parent or subsidiary company of the Service Provider, approved in accordance with Clause 5, provided that the Service Provider and that parent or subsidiary company have adopted Binding Corporate Rules which have been approved by the relevant national data protection supervisory authority under Article 47 of the GDPR.

6.3 For the purposes of Clause 6.2.2 above, the parties to the Standard Contractual Clauses shall undertake and document a risk assessment on the laws and practices in force within the country outside the EEA where the data importer is located (a 'Transfer Impact Assessment'), and where necessary implement supplementary measures. Where the Service Provider, and not the HSE, is acting as the data exporter, the Service Provider shall, upon request, make available to the HSE a copy of the Transfer Impact Assessment, and provide details of any supplementary measures implemented.

6.4 For the purposes of Clause 6.2.3 above, the Service Provider and the transferee in the country outside the EEA, shall undertake and document a Transfer Impact Assessment, and where necessary implement supplementary measures. The Service Provider shall, upon request, make available to the HSE a copy of the Transfer Impact Assessment, and provide details of any supplementary measures implemented.

6.5 Upon the written request of the HSE, the Service Provider shall supply the HSE within 14 calendar days, with a complete list of all countries around the world, where the Service provider and (as applicable) their Sub-Processors are currently processing HSE Personal Data.

6.6 In the event that the transfer mechanism entered into under this Clause 6 of this Agreement ceases to be valid, the Service Provider shall at the HSE's discretion:

6.6.1 Enter into and/or procure that any relevant Sub-Processor enters into an appropriate alternative data transfer mechanism;

6.6.2 Delete any HSE Personal Data in its and/or its Sub-Processor's possession; or

6.6.3 Return any HSE Personal Data in its and/or its Sub-Processor's possession to the HSE;

6.7 In the event that there ceases to exist any valid data transfer mechanism which would enable the Personal Data to be lawfully transferred by the HSE to the Service Provider, the HSE shall be entitled to terminate the Contract(s) forthwith.

7 Personal Data Breach

7.1 The Service Provider shall notify the HSE without undue delay, and at the latest within 72 hours, after the Service Provider or (as applicable) their Sub-Processors become aware of a Personal Data Breach within their respective organisations which affects any HSE Personal Data which is Processed by the Service Provider or (as applicable) their Sub-Processors;

7.2 When notifying the HSE of a Personal Data Breach, the Service Provider shall ensure the notification includes, at a minimum, the information listed in Article 33(3) of the GDPR.

8 Audit

8.1 The Service Provider shall keep accurate and up-to-date records relating to its Processing of HSE Personal Data;

8.2 At no additional cost to the HSE, the Service Provider shall make available to the HSE all information necessary to demonstrate the Service Providers compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the HSE or, subject to the Service Providers consent, another auditor mandated by the HSE. If and when the HSE decides to exercise its rights under this provision, the HSE and the Service Provider agree to negotiate in good faith the scope and implementation details of this provision. Without prejudice to the foregoing, any such audits or inspections shall be carried out under a duty of confidentiality, on reasonable written notice and during regular business hours and shall not unreasonably interfere with the Service Provider's business activities.

9 Termination or Completion of Agreement

9.1 Without affecting indemnity, other right or remedy available to the HSE, a breach by the Service Provider of any of the terms of this Agreement shall be deemed a material breach and where that breach is irremediable or if such breach is remediable and the Service Provider fails to remedy that breach within 30 calendar days after being notified by the HSE to do so, then the HSE may terminate any Contract(s) it has with the Supplier with immediate effect by giving written notice to the Service Provider.

9.2 Upon termination or the completion of any Contract(s), the Service Provider shall, at the request and choice of the HSE, Delete or return to the HSE, all HSE Personal Data held by the Service Provider and (as applicable) their Sub-Processors:

9.2.1 Where the HSE has requested the Service Provider Delete the HSE Personal Data, the Service Provider shall ensure all HSE Personal Data and all the copies thereof (irrespective of format) held by the Service Provider and (as applicable) their Sub-Processors is Deleted from all of the Service Provider's and (as applicable) their Sub-Processors' IT systems, IT devices, mobile computer devices, removable storage devices and Servers within 30 calendar days. The Service Provider shall notify the HSE in writing, when they and (as applicable) their Sub-Processors have completed the Deletion process;

9.2.2 Where the HSE has requested the Service Provider return the HSE Personal Data, the Service Provider shall ensure all HSE Personal Data and all the copies thereof (irrespective of format) held by the Service Provider and (as applicable) their Sub-Processors is returned to the HSE within 30 calendar days. The Service Provider shall ensure all HSE Personal Data held electronically by the Service Provider and (as applicable) their Sub-Processors is returned to the HSE in a commonly used electronic format;

9.2.3 In circumstances where, after the termination or completion of any Contracts, the Service Provider is required under European Union or Irish Law to retain a copy of any HSE Personal Data, the Service Provider undertakes to supply the HSE in writing, unless prohibited by law, with the full details of any HSE Personal Data

they are legally required to retain and the details of the European Union or Irish Law governing this requirement. In such circumstances, the Service Provider shall ensure all HSE Personal Data is appropriately secured and encrypted at all times to a standard which is satisfactory to the HSE and shall ensure that the HSE Personal Data is only processed for the specific legal retention purpose so-notified to the HSE. When the Service Provider is no longer legally required to retain the HSE Personal Data, the Service Provider shall, at the request and choice of the HSE, Delete or return to the HSE, the HSE Personal Data in accordance with Clauses 9.2.1 and 9.2.2 of this Agreement.

9.3 Upon termination or the completion of any Contract(s), the Service Provider shall return to the HSE with immediate effect, all HSE IT devices, mobile computer devices, removable storage devices, phones, parking permits, I.D. badges and any other equipment which the HSE provided to the Service Providers employees and contractors.

10 Indemnity. Notwithstanding any other provision of the Contract(s), The Service Provider hereby indemnifies and holds harmless, and agrees to keep indemnified and hold the HSE harmless against all damages, losses, liabilities, costs, fines and/or penalties, expenses, compensation and associated costs arising out of or in connection with any act, omission, default or negligence of the Service Provider and its Sub-Processors relating to the Processing of HSE Personal Data under this Agreement.

11 Survival of Obligations. All the obligations under this Agreement will survive and continue after termination, and will bind the Service Provider's legal representatives, successors and assigns until such time as all the HSE Personal Data has been returned to the HSE or permanently destroyed.

12 Waiver. The rights of the HSE under this Agreement will not be prejudiced or restricted by any indulgence or forbearance extended to the Service Provider or other parties, and no waiver by the HSE in respect of any breach of the terms of this Agreement will operate as a waiver in respect of any subsequent breach.

13 Variation

13.1 Subject to Clause 13.2, this Agreement may not be released, discharged, supplemented, amended, varied or modified in any manner except by an instrument in writing signed by a duly authorised officer or representative of each of the parties hereto**;**

13.2 The HSE may amend this Agreement if there is any change to the Data Protection Legislation which necessitates changes to this Agreement, and this Agreement as so amended shall be binding on the parties hereto.

14 Notice. Any notice or other communication given or made under this Agreement shall be in writing and may be sent by email, delivered to the relevant party, or sent by pre-paid registered post airmail to the address of that party specified in this Agreement or such other address as may be notified hereunder by that party from time to time for this purpose and will be effective notwithstanding any change of address not so notified. Unless the contrary is proved, each such notice or communication will be deemed to have been given or made and delivered, if by email

upon delivery, if by post 48 hours after posting, or if by delivery when left at the relevant address.

15 **Severance.** If any provision of this Agreement is found by any court or administrative body of competent jurisdiction to be invalid, unenforceable or illegal, the other provisions of this Agreement will remain in force. If any invalid, unenforceable or illegal provision would be valid, enforceable or legal if some part of it were deleted, the provision will apply with whatever modification is necessary to make it valid, enforceable or legal.

16 **Conflicts.** With regard to the Processing of HSE Personal Data, in the event of any conflicts or inconsistency between the terms of this Agreement and the Contract(s), the terms of this Agreement shall prevail.

17 **Counterparts.** This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Transmission of the executed signature page of a counterpart of this Agreement by email (in PDF, JPEG or other agreed format) shall take effect as delivery of an executed counterpart of this Agreement. If such method of delivery is adopted, without prejudice to the validity of this Agreement, each party shall provide the other with the original of such counterpart as soon as reasonably possible thereafter**.**

18 **Assignment.** The Service Provider cannot, without the prior written consent of the HSE, assign, sublicense, subcontract, mortgage or otherwise transfer or dispose of the whole or any part of this Agreement.

19 **Further Assurance.** Each Party undertakes to do all acts and execute all documents which may be necessary to give full effect to this Agreement.

20 **Further Assistance.** Each Party shall cooperate with and provide assistance to the other Party consistent with the terms and conditions of this Agreement.

21 **Governing Law.** This Agreement will be governed by and construed in accordance with the laws of Ireland and the parties hereto hereby irrevocably submit to the exclusive jurisdiction of the courts of Ireland.

IN WITNESS where of this Agreement has been entered into the day and year first herein written.

SIGNED on behalf of the **Health Service Executive**	**In the presence of**
…..... Signature	…..... Signature
…..... Name (printed)	…..... Name (printed)
….....……. Title	…..... Title
Date: …….....	Date: …….....
SIGNED on behalf of ……. **(**the **Service Provider)**	**In the presence of**
…..... Signature	…..... Signature
…..... Name (printed)	…..... Name (printed)
…..... Title	…..... Title
Date: …….....	Date: …….....

Appendix 1

The data processing activities carried out by the Service Provider pursuant to the Agreement are described as follows:

1. Subject Matter of the Processing

The Service Provider is under Contract(s) to provide one or more Services to the HSE. The provision of these Services to the HSE necessitates the Service Provider Processing data including Personal Data on behalf of the HSE.

2. Duration of the Processing

The HSE Personal Data shall be Processed by the Service Provider for as long as necessary. The duration of the Processing shall correspond to the terms of the Contract(s) for the Services between the Service Provider and the HSE.

3. Nature and Purpose of the Processing

The Service Provider shall only Process Personal Data as necessary to provide the Services pursuant to the Contract(s) between the HSE and the Service Provider, this Agreement and as further instructed by the HSE.

Depending on the Service(s) provided by the Service Provider to the HSE, the Personal Data may be subject to the following basic Processing activities

- Receive data, including collection, accessing, retrieval, recording and data entry.
- Hold data, including storage, hosting, organisation and structuring.
- Use data, including analysing, consultation, migrating and testing.
- Update data, including correcting, adaptation, alteration, alignment and combination.
- Send data, including electronic transmission and sending by other means.
- Protect data, including restricting, encrypting, and security testing.
- Share data, including disclosure, dissemination, allowing access or otherwise making data available.
- Backup data, including taking, storing and restoration of data.
- Erase data, including destruction and deletion.

4. Description of the HSE Personal Data (if applicable) processed

Depending on the Service(s) provided by the Service Provider to the HSE, the Service Provider whilst providing the Service(s) to the HSE, may Process the following categories of Personal Data & Special Categories of Personal Data:

Personal Data, which may include, but is not limited to the following:

- First and Last name
- Title
- Position
- Date of Birth
- Home contact details (address, telephone number, mobile number, personal email address)
- Business contact details (address, telephone number, mobile number, personal email address, work location)
- Family life
- Civil Partnership and Marital status
- Employer name & address
- Employee number
- Personal Public Service Number (PPSN)
- Individual Health Identifier (IHI)
- Medical Record Number (MRN)
- Personal life data
- Professional life data
- Connection data
- Location data
- Financial and bank details
- Employment details
- Education details
- General Practitioner contact details (name, address, contact telephone number)

Special Categories of Personal Data, which may include, but is not limited to the following:

- Racial or Ethnic origin
- Religious or philosophical beliefs
- Trade union membership
- Data concerning health
- Sex life or sexual orientation
- Biometric data
- Genetic data

5. Categories of Data Subjects who's Personal Data is processed

Depending on the Service(s) provided by the Service Provider to the HSE, the Service Provider whilst providing the Services to the HSE, may Process Personal Data relating to the following categories of Data Subjects:

- HSE staff and contractors
- HSE Agency staff and contractors
- HSE patients, clients and service users

- HSE Agency patients, clients and service users
- HSE business partners, service providers and suppliers (who are natural persons)
- HSE business partners, service providers and suppliers staff and contractors (who are natural persons)
- Individuals seeking employment with the HSE and/or HSE Agencies
- Retired HSE or HSE Agency staff

Appendix 2

List of Sub-Processors currently engaged by the Service Provider and approved by the HSE to Process the HSE Personal Data or any part thereof the Personal Data.

Sub-Processor (Company name, location etc.)	**Function** (Type of service(s) provided by the sub-processor)	**Processing location** (Geographic location where processing takes place)

Appendix 3

The minimum technical and organisational measures that must be implemented by the Service Provider when using their own ICT resources to Process HSE Personal Data:

1. All IT Networks (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store any HSE Personal Data have properly managed, configured and up to date firewalls in place;

2. All IT Networks (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data have properly managed and configured network monitoring and logging in place;

3. All IT Networks (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data have properly managed, configured and up to date intrusion detection and/or intrusion prevention systems in place;

4. All IT Networks (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data have strong access controls in place;

5. Appropriate levels of network, system, and physical redundancy are in place;

6. All the buildings or facilities (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to host IT systems, IT devices, Servers and other critical IT equipment which are used to Process or store HSE Personal Data are protected by appropriate physical and environmental controls;

7. All IT devices, mobile computer devices and Servers (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data have real-time protection anti-virus, anti-malware and anti-spyware software installed and updated daily;

8. All IT systems, IT devices, mobile computer devices, Servers and other critical IT equipment (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data are protected by strong unique passwords which satisfy or better the requirements of the HSE Password Standards Policy (https://www.hse.ie/eng/services/publications/pp/ict/);

9. All the mobile computer devices and removable storage devices (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data have encryption enabled which encrypts any HSE Personal Data stored at rest on the device. The encryption of the HSE Personal Data on the device may be achieved by either full-disk encryption, file system encryption or (as applicable) database encryption. All encryption used by the Service Provider must satisfy or better the requirements of the HSE Encryption Policy (https://www.hse.ie/eng/services/publications/pp/ict/);

10. All Servers (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data have encryption enabled which encrypts any HSE Personal Data stored at rest on the Server. The encryption of the HSE Personal Data on the Server may be achieved by either full-disk encryption, file system encryption or (as

applicable) database encryption. All encryption used by the Service Provider must satisfy or better the requirements of the HSE Encryption Policy (https://www.hse.ie/eng/services/publications/pp/ict/);

11. All Servers (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data are backed up on a daily basis. Where the Service Provider backs up the Servers onto backup media, the Service Provider must ensure the following:

    11.1 The backup media is stored a sufficient distance away from the Server, for example, in another building on-site under the control of the Service Provider or off-site in a building or facility controlled by the Service Provider or a contracted third party;

    11.2 When not in use, the backup media is protected from damage caused by fire, heat, humidity, water and exposure to strong magnetic fields;

    11.3 The backup media is password protected by strong unique passwords which satisfy or better the requirements of the HSE Password Standards Policy (https://www.hse.ie/eng/services/publications/pp/ict/);

    11.4 The backup media is encrypted using strong encryption which satisfies or betters the requirements of the HSE Encryption Policy (https://www.hse.ie/eng/services/publications/pp/ict/);

    11.5 Access to the backup media is limited to the Service Providers employees, contractors and/or (as applicable) Sub-Processors who are involved in the backup process;

    11.6 When in transit, the backup media is protected at all times from damage, theft, interference and loss;

    11.7 The backup media is tested by the Service Provider on a regular basis;

    11.8 All old, obsolete and damaged backup media which was used to backup HSE Personal Data is physically destroyed.

12. All Servers (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data have logging enabled, and the Server logs are monitored by the Service Provider on a regular basis;

13. All HSE Personal Data which is sent in transit by the Service Provider is sent via secure channels (for example, VPN, Secure FTP or TLS) or encrypted email. All encryption used by the Service Provider must satisfy or better the requirements of the HSE Encryption Policy (https://www.hse.ie/eng/services/publications/pp/ict/);

14. Appropriate patch management procedures are in place for managing the timely application of relevant security software updates and patches to all IT devices, mobile computer devices, Servers

and other critical IT equipment (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data;

15. Documented disaster recovery plans are in place which detail how the Service Provider will restore the availability of, and access to any Servers (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data in the event of a physical or technical security breach;

16. Appropriate asset management procedures are in place which allow for the management and recording of all the Service Providers IT hardware and software assets used to Process or store HSE Personal Data;

17. Appropriate procedures are in place for the timely decommissioning and secure wiping or destruction (i.e. process that renders data unrecoverable) of all old, obsolete and damaged IT devices, mobile computer devices, Servers, software and other critical IT equipment (with the exception of those which are owned or controlled by the HSE) used by the Service Provider to Process or store HSE Personal Data;

18. Appropriate procedures are in place which allow the Service Provider to regularly, test, assess and evaluate the effectiveness of the technical and organisational measures they have implemented to ensure the security of HSE Personal Data which they Process on behalf of the HSE;

19. Appropriate separation controls are in place which provide for the separation of different customers data on the Service Providers IT hardware and software and ensure HSE Personal Data is Processed by the Service Provider as separately as possible from the Service Providers other customer's data;

20. Full separation (where applicable) of the Service Providers production and development / test / training environments is in place;

21. Documented IT and information security policies are in place which all the Service Provider's employees and contractors sign up to, and are expected to comply with;

22. Appropriate procedures are in place for the vetting of all new Service Provider employees and contractors who will have access to HSE Personal Data;

23. Non-disclosure and confidentiality clauses are included in the Service Providers contracts of employment for all their employees and contractors who have access to HSE Personal Data;

24. Where legally required to do so, the Service Provider has appointed a Data Protection Officer (DPO) in accordance with Article 37 of the GDPR.