Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

Service Provider Confidentiality Agreement



Version 3.0

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**)**)

This Agreement is an addendum to the ***HSE Standard Terms for Services & Supplies*** (and/or title of bespoke contract).

……..

……..
(Title of bespoke contract, the "Tender Contract" **(**Block Capitals**)**)

RECITALS

A. In connection with a current or proposed Service between the HSE and the Service Provider, whereby the Service Provider is supplying, or proposes to supply, goods or services (the **Service**) to the HSE, the HSE may directly make available to the Service Provider from time to time the *Information* (as defined below), or the Service Provider or its servants, employees, agents, affiliates, subsidiaries or sub-contractors may indirectly acquire or have access to the *Information* by virtue of the Service.

B. It is intended that this Agreement will govern the terms and conditions applying to the Service Provider's use of the *Information* and other related matters.

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

1 Definitions:

In this Agreement, unless the context otherwise requires:

Contact Data means personal data limited to the business contact details of any employee of the HSE or a HSE Agency who will communicate with Service Provider personnel regarding the *Service;*

Data Breach has the same meaning as "personal data breach" as set forth in Article 4 of the GDPR;

Data Controller or Controller has the meaning given to that term in Section 1(1) of the Data Protection Acts and (when effective) in Article 4 of the GDPR;

Data Processor or Processor has the meaning given to that term in Section 1(1) of the Data Protection Acts and (when effective) in Article 4 of the GDPR;

Data Protection Acts means the Data Protection Acts 1988 and 2003 (as amended) and the European Communities (Electronic Communications, Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336/2011) and every statutory modification, re-enactment, replacement and/or amendment thereof for the time being in force (or, where the context so admits or requires, any one or more of such Acts) and all orders and regulations/statutory instruments made thereunder;

Data Protection Directive means Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

Data Subject has the meaning given to this term in Section 1(1) of the Data Protection Acts;

Delete for the purposes of this agreement means removing all Information which is electronically held in such a way that it can never be retrieved from the device on which it is held;

FOIA 2014 means the Freedom of Information Act 2014 and any amendments to or replacements thereof, including by means of directly effective EU Regulation;

GDPR means the EU General Data Protection Regulation, Regulation (EU) 2016/679, the effective date of which is 25th May 2018. Provisions referencing GDPR in this Agreement will be applicable when the GDPR becomes effective;

Information means all information, (irrespective of the format, paper, electronic or otherwise) that is provided to the Service Provider by or on behalf of HSE in connection with the *Service*. *Information* may include *Personal Data* concerning HSE and HSE Agency clients, patients and staff, and confidential codes or any other information concerning the security of the HSE's ICT infrastructure, but shall exclude Contact Data*;*

Personal Data has the meaning given to that term in Section 1(1) of the Data Protection Acts and (when effective) in Article 4 of the GDPR, and relates only to personal data, or any part of such personal data, of which the HSE is the Data Controller or joint Data Controller and in relation to which the Service Provider is providing the Service, and includes Sensitive Personal Data and Special Categories of Data;

Processing and Process has the meaning given to those terms in Section 1(1) of the Data Protection Acts and (when effective) in Article 4 of the GDPR;

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

Sensitive Personal Data has the meaning given to this term in Section 1(1) of the Data Protection Acts;

Special Categories of Data has the meaning given to this term and/or such Personal Data as referred to in Article 9(1) and/or Article 10 of the GDPR.

Any reference to **third party** in this Agreement includes, for the avoidance of doubt, subcontractors.

2 Obligations of the Service Provider:

In consideration of the HSE directly making the *Information* available to the Service Provider, or the Service Provider otherwise acquiring the *Information*, and in consideration of the award of the Tender Contract, the Service Provider shall:

2.1 Not take or remove any *Information* from HSE premises without having received the written consent of the HSE. Such written consent must be issued in advance of the first instance and will apply thereafter;

2.2 Manage and *Process* any *Information* which they acquire from the HSE in accordance with the documented instructions of the HSE as set out in this Agreement and the obligations of the *Data Protection Acts* and the *GDPR* in so far as these obligations apply to a *Data Processor*, including with regard to transfers of *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 of that legal requirement before *Processing*, unless that law prohibits such information on important grounds of public interest;

2.3 Maintain secret and confidential all *Information* furnished to it or otherwise acquired by its servants, employees, agents, affiliates, subsidiaries or sub-contractors save and to the extent that such *Information* has been made available to the public by the HSE or by any third party lawfully in possession thereof and entitled to make such disclosure without restriction;

2.4 Take appropriate measures to ensure the reliability of the Service Providers servants, employees, agents, affiliates, subsidiaries or sub-contractors who have access to the Information;

The Service Provider must be in a position to provide the HSE with a named list of their servants, employees, agents, affiliates, subsidiaries or sub-contractors authorised to have access to *Information*.

2.5 Not disclose *Information* to any of the Service Provider's servants, employees, agents, affiliates, subsidiaries or sub-contractors unless and only to the extent that such persons need to know such *Information* for the purposes of providing services in connection with the *Service*, and provided that such person has been made aware of the restrictions in this Agreement on the disclosure of the *Information* and has agreed in writing to comply with such restrictions or materially similar restrictions;

2.6 Not disclose any *Information* to any third party without the prior written consent of the HSE unless the Service Provider is legally required to do so (see Clause 3.0 of this Agreement);

2.7 Not engage any third party to process the *Information* or any part thereof on its behalf without the prior written consent of the HSE. Should such consent be given, then the obligations of the Service Provider as set out in Clause 2 of this Agreement shall be imposed on that third party by way of a separate written agreement between the Service Provider and the third party, which agreement will terminate automatically upon termination of this Agreement for any reason. In the event that the third party fails to fulfil its obligations set out in Clause 2 of this Agreement, the Service Provider shall remain fully liable to the HSE for the performance by the third party of those obligations;

2.8 Not use the *Information* directly or indirectly for any purpose other than in connection with the provision of services to the HSE regarding the Service;

2.9 Not reverse engineer, de-compile or disassemble *Information* or attempt to use the *Information* in any form other than machine readable object code, or allow a third party to do any of the above;

2.10 Not make any press announcement or otherwise publicise the business relationship with the HSE in any way including, without limitation, using the name of the HSE in any publicity material, unless authorised to do so by the HSE;

2.11 Only use the *Information* solely for the purposes of fulfilling the requirements of the Service.

2.12 Take the necessary precautions for the prevention of unauthorised access to, unauthorised disclosure of or other unauthorised processing of the *Information* and in particular:

2.12.1 Keep all *Information* obtained from the HSE or otherwise relating to the Service separate from all documents and other records of the Service Provider. The HSE accepts that this requirement would be achieved by the Service Provider through logical electronic separation using role based access controls;

2.12.2 Only make such copies of the *Information* as are necessary for the provision of services to the HSE regarding the Service; and

2.12.3 Ensure that any notices related to the confidentiality or privacy of the *Information* provided by the HSE are not removed or altered; and

2.12.4 Have all necessary access controls in place to include authentication and authorisation for access to *Information* to ensure its security and confidentiality; and

2.12.5 Have all necessary systems in place to ensure the ongoing confidentiality, integrity, availability and resilience of *Processing* systems and services; and

2.12.6 Have the ability to restore the availability and access to the *Information* in a timely manner in the event of a physical or technical incident; and

2.12.7 Have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the *Processing* of the *Information*;

2.13 Ensure, upon termination or the completion of this Agreement, that all documents, data, other records or tangible objects containing or representing *Information* which have been disclosed by the HSE to the Service Provider ("***Information Records***"), and all copies thereof which are in the possession of the Service Provider and their subcontractors, shall at the written request and election of the HSE, be returned to the HSE or securely *Deleted*. Without prejudice to the generality of the foregoing:

2.13.1 Where the HSE has requested that the Service Provider return *Information Records*, the *Information Records* shall be returned from the Service Provider to the HSE in a commonly used electronic format;

2.13.2 Where the HSE has requested that the Service Provider securely *Delete Information*, the Service Provider shall ensure the Information is permanently *Deleted* from any of the Service Providers systems or devices which were used to store the *Information* and from those of third parties to whom the Service Provider has disclosed and/or permitted access to the *Information* or *Information Records*;

2.13.3 Where the Service Provider is required for for legal or regulatory compliance to retain a copy of any *Information*, the Service Provider shall provide the HSE in writing with full details of any *Information* they are proposing to retain and the details of the legal and regulatory obligations governing this action.

2.13.4 Without prejudice to the obligations at Clause 2.13.3 above, in circumstances where European Union or Irish law requires the Service Provider to retain any *Personal Data* which the HSE has shared with the Service Provider, the Service Provider shall provide the HSE in writing with full details of any *Personal Data* they are legally required to retain and the details of the European Union or Irish legal obligations governing this action, and ensure the *Personal Data* retained by them is anonymised or *Pseudonymised* by them to the HSE's satisfaction and in a manner and to a standard which is satisfactory under European Union law (including, without limitation, the *GDPR*);

2.14 Implement appropriate technical and organisational controls in accordance with Section 2(c) of the *Data Protection Acts* and Article 32 of the *GDPR*, to keep the *Information* secure and to protect against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the *Information* transmitted, stored or otherwise processed by the Service Provider;

2.15 Provide reasonable assistance to the HSE relating to its compliance with the provisions of Articles 33 to 36 of the *GDPR* and/or any legislative requirements of the *Data Protection Acts* or any guidance issued by the Irish Data Protection Commissioner;

2.16 Notify the HSE without undue delay, after they or (as applicable) their subcontractors become aware of a *Data Breach*. In the event of a Data Breach, the Service Provider will (a) investigate the *Data Breach*, (b) provide the HSE with all the relevant details surrounding the *Data Breach*, (c) provide the HSE with details of the measures taken or proposed to be taken by the Service Provider to mitigate the effects and to minimise any damage resulting from the *Data Breach*, and (d) assist the HSE in fulfilling its obligation to notify the relevant supervisory authority and *Data Subjects* of a *Data Breach* in accordance with Articles 33 and 34 of the *GDPR*;

2.17 Taking into account the nature of the processing, assist the HSE by appropriate technical and organisational measures, insofar as this is possible, to enable the HSE to fulfil its obligations to respond to requests from Data Subjects exercising their rights under Section 2D of the Data Protection Acts and Chapter III of the GDPR, (including the rights of access to, rectification of and erasure of their Personal Data), and shall promptly comply with any request from the HSE to amend, transfer or Delete such Personal Data.

2.18 For the purposes of Freedom of Information / transparency obligations placed upon the HSE (by *FOIA 2014* or otherwise):

2.18.1 Procure that it and its servants, employees, agents, subsidiaries or sub-contractors shall assist the HSE, at no additional charge and within such timescales as the HSE may reasonably specify, in meeting any requests for *Information* which are made to the HSE under the *FOIA 2014*, such assistance to include (but not be limited to) the provision of a copy of the requested *Information.*

2.18.2 Notwithstanding anything to the contrary in this Agreement, if the HSE receives a request for *Information* pursuant to the *FOIA 2014*, the HSE shall be entitled to disclose all *Information* (in whatever form) as is necessary to comply with the *FOIA 2014*.

2.18.3 If, at the request of the Service Provider, the HSE seeks to withhold *Information* protected by this Agreement and a competent authority determines, or the parties subsequently agree, that the *Information* is not exempt, then the Service Provider shall reimburse the HSE for all costs (including but not limited to legal costs) incurred by the HSE in seeking to withhold such *Information* from a request under the *FOIA 2014*.

2.18.4 Not (and shall procure that its servants, employees, agents, subsidiaries or sub-contractors do not) respond directly to a request for *Information* under the *FOIA 2014* unless expressly authorised to do so by the HSE.

2.19 Ensure the security of Information stored on all fixed and mobile devices, including medical devices, desktop computers, servers and mobile computer devices (i.e. laptops, notes, tablets, personal data assistants, Blackberry enabled devices, iPads, iPhones and other smart type devices etc) and removal storage devices (i.e. CD, DVD, portable hard drives, Diskettes, ZIP disks, Magnetic tapes etc).

2.19.1 Only in exceptional circumstances and with the written consent of the HSE, should the Service Provider hold *Information* on mobile computing or removable storage devices. Should the business requirements necessitate the holding of *Information* on such devices then the Service Provider shall ensure that only *Information* absolutely necessary for their purpose is stored in this format. The Service Provider will *Delete* or return all copies of the *Information* after the business requirements have been fulfilled, or earlier upon the written request of the HSE.

2.19.2 Where the use of mobile computing or removal storage devices is a necessity then the Service Provider will take all necessary precautions to ensure the safety of these devices from theft, loss and unauthorised access. As a minimum all mobile computing and removal storage devices must be appropriately secured including by means of strong encryption and protected by the use of strong complex passwords.

2.19.3 The encryption used by the Service Provider on the Service Providers laptops must satisfy or better the requirements of the *HSE Encryption Policy.* The current HSE encryption standard for laptop devices is Advanced Encryption Standard (AES) 256 (http://hse.ie/eng/services/Publications/pp/ict/Encryption_Policy.pdf). The HSE will notify the Service Provider of any relevant changes to the *HSE Encryption Policy*. At any time during the term of this Agreement the HSE may request the Service Provider to set out in writing the current encryption measures used and the Service Provider will provide this information within 5 days. If, in the reasonable opinion of the HSE, the encryption standard employed by the Service Provider is not sufficient, the Service Provider will implement, at their expense, whatever encryption standards are proposed by the HSE. At no time should cipher keys be held on the mobile computing or removal storage device for the data which they secure. In addition, the Service Provider will at all times hold cipher keys in a secure fashion.

2.19.4 Under no circumstances encrypted or otherwise is the Service Provider sanctioned by the HSE to download or store *Information* on USB memory sticks/keys.

2.20 Ensure the security of the *Information* in transit (including by way of electronic transit/ transit by way of electronic communication). Where it is necessary to transfer the *Information*, the Service Provider must take all necessary precautions to ensure the security of the *Information* before, during and after transit.

2.20.1 The Service Provider shall ensure that all transfers of the *Information* are legal, justifiable, and only the minimum *Information* absolutely necessary for a given purpose is transferred.

2.20.2 All transfers of *Information* should, where possible, only take place electronically via secure on-line channels or electronic mail. Where the Service Provider transfers *Information* electronically, in any form and by any means, the *Information* must be encrypted using strong encryption. The encryption methods used must satisfy or better the requirements of the *HSE Encryption Policy*. The current HSE encryption standard for electronic transfer is SSL (Secure Socket Layer) and TLS (Transport Layer Security) and Advanced Encryption Standard (AES) 256 in the case of encrypted email. The HSE will notify the Service Provider of any relevant changes to the *HSE Encryption Policy*.

2.20.3 Where it is not possible to transfer the *Information* electronically, the *Information* may be encrypted and copied to a mobile storage device (with the exception of USB memory sticks/keys) and transported manually. The encryption methods used must satisfy or better the requirements of the *HSE Encryption Policy*. The current HSE encryption standard for mobile storage devices is Advanced Encryption Standard (AES) 256. The HSE will notify the Service Provider of any relevant changes to the *HSE Encryption Policy*. Encrypted mobile storage media, should wherever possible, be hand delivered by the Service Provider to, and be signed for by, the intended recipient. If this is not possible, the use of registered post or some other certifiable delivery method must be used**.**

2.21 In relation to transfers of *Information* outside of the Republic of Ireland.

2.21.1 The Service Provider must seek the written consent of the HSE prior to the Service Provider transferring *Information* outside the jurisdiction of the Republic of Ireland. The HSE may, at its discretion, prohibit the Service Provider from transferring *Information* outside the jurisdiction of the Republic of Ireland.

2.21.2 Where the HSE has consented to the transfer of *Information* outside the Republic of Ireland, the Service Provider may only transfer *Information* to a legal entity located in:

2.21.2.1 A country within the European Economic Area;

2.21.2.2 A country outside the European Economic Area but approved for this purpose by the EU Commission pursuant to Article 25 of the Data Protection Directive and Article 45(3) of the GDPR;

2.21.2.3 A country outside the European Economic Area but subject to the execution by the HSE, the Service Provider and the transferee of standard data protection clauses adopted by the EU Commission in accordance with the examination procedure referred to in Article 31(2) of the *Data Protection Directive* (and Article 93(2) of the *GDPR*), as provided for in Article 26(4) of the *Data Protection Directive* (and Article 46 of the *GDPR*);

2.21.2.4 A country outside the European Economic Area but where the transferee of the Information is a parent or subsidiary company of the Service Provider, 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 Authority under Article 26(2) of *Data Protection Directive* and/or the comply with the provisions of Article 47 of the *GDPR*;

2.21.2.5 The United States of America only when the *Information* transferee has agreed in writing to be bound by the European Commission's Implementing Decision (EU) 2016/1250 of 12th July 2016 (EU-US Privacy Shield).

2.22 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 another auditor mandated by the HSE. The Service Provider and the HSE agree to negotiate in good faith the scope and implementation details of this provision at the time the HSE decides to exercise its rights under this provision.

3 Disclosure Required by Law: In the event that the Service Provider is legally required to disclose any of the *Information* 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.

The Service Provider must co-operate with the HSE in bringing any legal or other proceedings to challenge the validity of the requirement to disclose Information.

4 **Breach of Agreement**: The Service Provider hereby indemnifies and agrees to keep indemnified the HSE against any costs, expenses, damages, harm or loss suffered or incurred by reason of any disclosure of the *Information* in breach of the terms and conditions of this Agreement and shall account to the HSE for any moneys received by the Service Provider directly or indirectly arising out of the disclosure or use of any of the Information in breach of the terms and conditions of this Agreement.

5 **No Warranty:** Nothing in this Agreement shall constitute a warranty by the HSE as to the accuracy of any of the *Information*, and the HSE will not be liable to the Service Provider or to any other party to which any of the Information may be disclosed for any loss or damage howsoever caused, arising directly or indirectly out of the inaccuracy of any of the Information.

6 **No Licence**: The Service Provider acknowledges that the Information is of a special and unique character and that the *Information* and any patent, copyright or other intellectual property rights of whatever nature attaching thereto are and will remain the property of the HSE and nothing in this Agreement will be construed as giving the Service Provider a licence in respect of such patent, copyright or other intellectual property rights.

7 **Survival of Obligations**: The non-disclosure obligations of this Agreement will survive and continue and will bind the Service Provider's legal representatives, successors and assigns notwithstanding that the Service may not be actually implemented by the parties.

8 **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.

9 **Variation:** 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**.**

10 **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 or fax to the address of that party specified in this Agreement or to that party's fax number thereat or such other address or number as may be notified hereunder by that party from time to time for this purpose and will be effective notwithstanding any change of address or fax number 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, if by delivery when left at the relevant address or, if by fax upon transmission, subject to the correct code or fax number being received on the transmission report.

11 **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.

12 **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

SIGNED on behalf of

In the presence of

…….
(the **Service Provider)**

…..
Signature

…..
Signature

…..
Name (printed)

…..
Name (printed)

…..
Title

…..
Title

Date: ……..... Date: …….....