St James's Hospital, James Street, Dublin 8. D08 NHY1
Ospidéal San Séamas, Sráid Shéamais, Baile Átha Cliath 8
+353 1 4103000 generalenquiries@stjames.ie www.stjames.ie
Registered Charity Number: 20017583

ST JAMES'S HOSPITAL

Data Processing Terms for Services provided to St James's Hospital

(Data Controller to Processor)

BETWEEN:

1. **St James's Hospital** registered in Ireland with company number 0085963R whose registered office is at PO Box 580 James's Street, Dublin 8 (the "**Data Controller**"); and

2. **Vendor** providing services to St. James' Hospital (the "**Data Processor**")

(each a "**Party**" and collectively the "**Parties**").

RECITALS:

A. The Parties have agreed to these terms in order to facilitate the provision of services by one Party to the other Party and to the extent that the provision of such services involves the processing of Personal Data and/or Special Categories of Data, for the purposes of ensuring compliance with Data Protection Laws (defined below).

B. The Parties agree to Process such Personal Data and Special Categories of Data in accordance with and subject to the terms and conditions hereafter appearing.

OPERATIVE TERMS:

The Parties agree as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 These terms (including the Recitals), unless the context otherwise requires, shall have the following meanings:

"**Data Protection Laws**"	means: (i) the data protection and information privacy laws of Ireland and the European Union; (ii) to the extent applicable to these terms or the Services and the Data Protection Laws of other jurisdictions; (iii) and includes any legislation in force from time to time which implements Directive 95/46/EC or Directive 2002/58/EC of the European Community the Data Protection Acts 1988, 2003 (as amended) & 2018, and any replacement regulation including the General Data Protection Regulation (as defined below);
"**Effective Date**"	means the date data processing commences;
"General Data Protection Regulation"	means Regulation (EU) 2016/679, known as the General Data Protection Regulation (the "**GDPR**");
"Law"	means any constitution, law, treaty, statute, ordinance, code, rule, regulation, executive order, administrative order or other order, judgment or determination of any Governmental Authority, Regulatory Requirement, applicable principle of common or civil law, or any binding

	agreement with any Governmental Authority, as amended from time to time within the scope of these terms;
"Personal Data"	has the meaning as set out in Data Protection Laws.
"**Services**"	means any services provided by the Data Processor to the Data Controller under these terms and/or any agreement entered into between the Data Processor and Data Controller including but not limited to past and future agreements; and
"Special Categories of Data"	has the meaning as set out in Data Protection Laws.

1.2 In these terms:

1.2.1 the clause headings are included for convenience only and shall not affect the construction of these terms;

1.2.2 words denoting the singular shall include the plural and vice versa and words denoting any gender shall include a reference to each other gender;

1.2.3 a reference to writing or written includes faxes and e-mail;

1.2.4 any obligation in these terms on a person not to do something includes an obligation not to agree, allow, permit or acquiesce in that thing being done;

1.2.5 where the words include(s), including or in particular are used in these terms, they are deemed to have the words without limitation following them. Where the context permits, the words other and otherwise are illustrative and shall not limit the sense of the words preceding them;

1.2.6 references to persons shall be deemed to include references to natural persons, firms, partnerships, companies, corporations, associations, organisations, foundations and trusts (in each case whether or not having separate legal personality); and

1.2.7 references in these terms to statutory provisions shall (where the context so admits and unless otherwise expressly provided) be construed as references to those provisions as respectively amended, consolidated, extended or re-enacted during the term of these terms (as the context requires) and to any orders, regulations, instruments or other subordinate legislation made under the relevant statutes.

2. APPOINTMENT AND TERM

2.1 Any capitalised terms used in these terms (including the Recitals) that are not defined will have the meaning given to them in Data Protection Laws.

2.2 The sole purpose of these terms is to deal with the effects of the Data Protection Laws and to ensure compliance with Data Protection Laws where the Personal Data and Special Categories of Data of Data Subjects is shared by the Parties. It does not purport to implement any other contractual terms in respect of the relationship between the Parties, nor to amend any such terms as may exist at the commencement of data processing **PROVIDED THAT** if, and to the extent that, any other contractual terms that have been agreed, or may in future be agreed, between the Parties conflict with these terms, these terms shall prevail except where such contractual terms are specifically expressed to vary on these terms.

2.3 The purpose of these terms is to describe the terms and conditions which govern the appointment of **Vendor** as Data Processor in respect of the Processing of Personal Data and Special Categories of Data on behalf of St James's Hospital, the Data Controller.

2.4 The Data Processor acknowledges and agrees that it will receive and Process certain Personal Data and Special Categories of Data (collectively referred to as Personal Data hereafter), details of which are set out in writing between the parties, in order and for as long as is necessary to perform its obligations under these terms.

2.5 These terms shall come into effect on the commencement of the data processing and shall continue in force unless and until terminated by either Party.

3. DATA PROCESSING

3.1 The Data Processor shall ensure that its internal operating systems only permit properly authorised personnel to access Personal Data.

3.2 The Data Processor shall provide appropriate training to its personnel with respect to:

(i) the correct handling of Personal Data so as to minimise the risk of security breaches; and

(ii) the requirements of the applicable Data Protection Laws.

3.3 The Data Processor acknowledges and agrees that it will:

(i) only Process Personal Data in accordance with the Data Controller's written instructions including with regard to transfers of personal data to a Third Country or an international organisation (which may be specific instructions or instructions of a general nature as set out in the terms or as otherwise notified by the Data Controller to the Data Processor from time to time and the Data Controller shall ensure it gives only lawful written instructions);

(ii) only use, reproduce or otherwise Process any Personal Data collected in connection with providing the Services to the extent necessary to provide the Services;

(iii) not modify, amend or alter the contents of the Personal Data, except as directed by the Data Controller;

(iv) not, without the Data Controller's written approval, Process any Personal Data on any Data Processor systems on which data (including any Personal Data) is Processed for any person outside of the Data Controller; and

(v) implement and maintain a system for logging and identifying all Data Processor personnel accessing any Personal Data through Data Processor systems and if requested by the Data Controller, the Data Processor shall provide to the Data Controller a copy of the access log.

3.4 The Data Processor shall implement appropriate technical and organisational measures (in particular those required under the GDPR) to assure a level of security appropriate to the risk to the security of Personal Data, in particular, from accidental or unlawful destruction, loss, alteration, unauthorised, disclosure of or access to Personal Data in accordance with the Data Processor's obligations under Data Protection Laws (the "**Security Measures**"). The Security Measures may also include as appropriate:

(i) the pseudonymisation and encryption of Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity and availability of the Personal Data and resilience of the Data Processor systems used for such Processing;

(iii) the ability to restore the availability and access to the Personal Data, in a timely manner but no later than forty eight (48) hours, in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.5 The Data Controller may notify the Data Processor immediately in the event that it does not consider that the Security Measures ensure an appropriate level of security for Personal Data and the Data Controller shall notify the Data Processor of any additional or amended security controls or measures which the Data Controller considers in its reasonable opinion is necessary to ensure compliance with Data Protection Laws. The Data Processor agrees to implement such additional security controls or measures.

3.6 The Data Processor agrees and warrants that the Security Measures are appropriate to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Personal Data to be protected having regard to the state of the art and the cost of their implementation.

3.7 Without limiting the Data Processor's other obligations under this Clause 3.7, the Data Processor:

(i) may disclose Personal Data to its personnel but only those who:

a) need to know for the purpose of providing the Services (and only to that extent);

b) have been trained in accordance with Clause 3.2;

c) are subject to a binding contract to keep the Personal Data confidential (or are under an appropriate statutory obligation of confidentiality), and

(ii) may only disclose Personal Data to any other person with the prior written consent of the Data Controller, and, where the Data Controller provides its consent, only where the person is subject to a binding commitment to keep the Personal Data confidential (or are under an appropriate statutory obligation of confidentiality).

3.8 If the Data Processor or Data Processor personnel are required by Law and/or an order of any court or competent jurisdiction or any regulatory, judicial or governmental body to disclose the Personal Data, the Data Processor shall, except where prohibited by Law, first:

(i) give the Data Controller notice of the details of the proposed disclosure;

(ii) give the Data Controller a reasonable opportunity to take any steps it considers necessary to protect the confidentiality of the Personal Data including but not limited to seeking such judicial redress as the Data Controller may see fit in the circumstances;

(iii) give any assistance reasonably required by the Data Controller to protect the confidentiality of the Personal Data; and

(iv) inform the proposed disclosee that the information is confidential.

3.9 Without limiting the Data Processor's other obligations under these terms, the Data Processor shall not engage any third-party processors to Process Personal Data without the prior written consent of the Data Controller. If the Data Processor engages any third party to Process any Personal Data, the Data Processor shall impose on such third party, by means of a written contract, the same data protection obligations as set out in these terms.

3.10 The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of the any third-party processors and shall not make any such changes without the prior written consent of the Data Controller.

3.11 The Data Processor shall remain liable to the Data Controller for Processing by such third parties as if the Processing was being conducted by the Data Processor.

3.12 The Data Processor acknowledges and agrees that the Data Processor or Data Processor personnel may not transfer Personal Data to any Third Country except to the extent that the transfer is expressly approved by the Data Controller in writing. If personal data processed under these terms is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data is adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

Assistance

3.13 Each Party shall co-operate with the other party to the extent necessary to enable that party to comply with any requests of the Office of the Data Protection Commissioner or other competent Supervisory Authority in respect of the Personal Data.

3.14 The Data Processor shall:

(i) make available to the Data Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Data Controller or another auditor mandated by the Data Controller;

(ii) immediately inform the Data Controller if, in its opinion, an instruction given, or request made pursuant to Clause 3.14 (i) infringes Data Protection Laws;

(iii) taking into account the nature of the Processing, provide such co-operation and assistance including by using appropriate technical and organisational measures as the Data Controller may require for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III of the GDPR;

(iv) provide such co-operation and assistance as the Data Controller may require to enable the Data Controller to comply with its obligations and in particular those obligations under Articles 32-36 of the GDPR including without limitation to notify the Data Controller without undue delay and in any event within twenty four (24) hours following the Data Processor becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data ("**Personal Data Breach"**). The Data Controller shall without undue delay notify the Data Processor of any Personal Data Breach affecting the Data Processor;

(v) immediately notify the Data Controller of any monitoring activities and measures undertaken by the Data Protection Authority that supervises the applicable Data Protection Laws;

(vi) support the Data Controller regarding the Data Controller's obligations to provide information about the collection, processing or usage of Personal Data to a Data Subject;

(vii) deal promptly and properly with all inquiries from the Data Controller relating to its Processing of the Personal Data and Special Categories of Data;

(viii) if the Data Processor receives any request by any person to access or correct Personal Data, the Data Processor shall, within two (2) Business Days, notify the Data Controller and provide the Data Controller with the full details of that request; and

(ix) ensure that the Personal Data are not in any way used, manipulated, distributed, copied or processed for any other purpose than for the fulfilment of the contractual obligations as explicitly agreed upon and arising from these terms.

Audit

3.15 The Data Processor shall maintain proper records of any Personal Data recovered from or on behalf of the Data Controller and of all training carried out with regard to the technical and organisational data Security Measures.

3.16 The Data Processor shall permit the Data Controller or its representatives to access all relevant systems (including the Data Processor systems), personnel, records and information of the Data Processor during normal working hours for the purpose of inspecting, testing and auditing the technical and organisational data Security Measures operated by the Data Processor and for the purpose of confirming the Data Processor's compliance with its obligations under these terms and with Data Protection Laws. The Data Processor shall promptly implement any requirement made by the Data Controller to improve the technical and organisation measures.

Information Obligations

3.17 If the Data Processor cannot provide compliance or foresees that it cannot comply with its obligations as set out in these terms, for whatever reasons, it agrees to promptly inform the Data Controller of its inability to comply, in which case the Data Controller is entitled to suspend the transfer of Data.

3.18 The Data Processor will promptly notify the Data Controller about:

(i) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental, unauthorised access, or other event that constitutes a Personal Data Breach; and

(iii) any request received directly from the Data Subjects without responding to that request, unless it has been otherwise authorised to do so.

Indemnity

3.19 The Data Processor shall indemnify the Data Controller, its directors, officers, agents, employees against any and all losses, expenses (including reasonable legal fees), damages, costs, penalties and losses incurred by the Data Controller or any of the Data Controller's personnel, arising from or in connection with the Data Processor acting outside or contrary to the lawful instructions of the Data Controller and/or any other breach by the Data Processor of its obligations under these terms or Data Protection Laws.

Return or Destruction of Personal Data

3.20 The Data Processor shall, at any time, on request by the Data Controller:

(i) not use, copy disclose or otherwise Process any Personal Data and promptly return the Personal Data to the Data Controller; and

(ii) if requested by the Data Controller, securely destroy all copies of the Personal Data received and/or processed by it under these terms unless Law requires storage of the Personal Data.

4. AMENDMENTS

4.1 In the event that the Data Protection Laws are amended or replaced by subsequent legislation or regulations or in the event that case law or findings of the relevant Data Protection Authority pursuant to the Data Protection Laws require amendments to these terms, in the reasonable opinion of the either Party then the other Party shall agree to such amendments to these terms and will enter into a deed of variation to effect such amendments.

5. TERMINATION

5.1 The Parties agree that on the termination of the Services, the Data Processor and any Sub-Processors shall return all the Personal Data transferred including any data storage media supplied to the Data Processor, and the copies thereof to the Data Controller or shall delete all the Personal Data and certify to the Data Controller that it has done so, unless legislation imposed upon the Data Processor prevents it from returning or deleting all or part of the Personal Data transferred.

6. COSTS AND EXPENSES

6.1 The Parties shall pay its own costs, charges and expenses incurred in relation to the preparation, execution and carrying into effect of these terms.

7. WAIVER

7.1 A failure by either Party to exercise and any delay, forbearance or indulgence by either Party in exercising any right, power or remedy under these terms shall not operate as a waiver of that right, power or remedy or preclude its exercise at any subsequent time or on any subsequent occasion. The single or partial exercise of any right, power or remedy shall not preclude any other or further exercise of that right, power or remedy. No custom or practice of the Parties at variance with the terms of these terms shall constitute a waiver of the rights of either Party under these terms.

8. NOTICES

8.1 Any notice required to be given under these terms shall be in writing and shall be served if hand delivered or sent by prepaid recorded or special delivery post or prepaid international recorded airmail to the address and for the attention of the relevant Party set out in Clause 8.2 or at such other address as either Party may designate from time to time in accordance with this Clause.

8.2 The addresses of the Parties for the purposes of written notices are:

(i) Data Controller:

Data Protection Officer
St. James's Hospital
Dublin 8
dataprotection@stjames.ie

(ii) **Vendor** business address.

or such other address as may be notified in writing from time to time by the relevant Party to the other. Any such change to the place of service shall take effect immediately after notice of the change is received or (if later) on the date (if any) specified in the notice as the date on which the change is to take place.

8.3 Any notice sent pursuant to this Clause 8 shall be deemed to have been served if hand delivered or sent by prepaid recorded or special delivery post or prepaid international recorded airmail, at the time of delivery.

9. FURTHER ASSURANCE

Each Party shall do and execute, or arrange for the doing and executing of, each necessary act, document and thing reasonably within its power for the purpose of giving full effect to these terms.

10. SEVERABILITY

If any Clause or part of these terms is found by any court, tribunal, administrative body or authority of competent jurisdiction to be illegal, invalid or unenforceable then that provision will, to the extent required, be severed from these terms and will be ineffective without, as far as is possible, modifying any other Clause or part of these terms and this will not affect any other provisions of these terms which will remain in full force and effect, unless the substantive purpose of these terms is then frustrated, in which case either Party may terminate these terms on written notice to the other.

11. ENTIRE AGREEMENT

These terms constitute an agreement between the Parties with respect to the subject matter unless otherwise agreed to in writing.

12. VARIATIONS

No variation of these terms shall be effective unless made in writing, expressed to be a variation of these terms and signed by or on behalf of each of the Parties.

13. COUNTERPARTS

These terms may be executed in any number of counterparts, each of which so executed will be an original, but together will constitute one and the same instrument.

14. GOVERNING LAW AND JURISDICTION

These terms are governed by and shall be construed in accordance with the laws of Ireland. The courts of Ireland have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with these terms and, for these purposes, each Party irrevocably submits to the exclusive jurisdiction of the courts of Ireland.

The Vendor agree to these terms when carrying out data processing on the instruction of St. James's Hospital (the Data Controller).