DATA PROCESSING AND CONFIDENTIALITY AGREEMENT

THIS AGREEMENT made on the 19th day of March 2020 BETWEEN:

(1) The Health Services Executive, represented by the Saolta Cancer Managed Clinical & Academic Network (hereinafter the "Data Controller") of the one part; and

(2) NATIONAL UNIVERSITY OF IRELAND, GALWAY, having a business address at University Road, Galway, Ireland (hereinafter called the "Data Processor") of the other part.

Each a "Party" and collectively known as the "Parties".

NOW IT IS HEREBY AGREED in consideration of the sum of €1.00 (the receipt of which is hereby acknowledged by the Data Processor) as follows:

1. Introduction

1.1 This agreement re processing of personal data (the **"Agreement**") regulates **NUI Galway and its representatives** processing of personal data on behalf of the Health Services Executive and/or Saolta Cancer, Managed Clinical and Academic Network (and Saolta and the Galway University Hospital). This Agreement also regulates the Data Processors use of any Confidential Information which comes into the Data Processors possession.

2. Legislation

2.1 This Agreement shall ensure that the Data Controller and the Data Processor complies with the applicable data protection and privacy legislation (the "Applicable Law"), including in particular the **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679).

3. Processing of personal data

3.1 Purpose: The purpose of the processing is the provision of the Services by the Data Processor to support the running and support of the Cancer, Managed Clinical & Academic Network (CMCAN) Biobank the purpose of which is to support the delivery of high-quality clinical care in an environment of research, education, training and innovation that together form key components for any Cancer care centre (the "Services").

3.2 In connection with the Data Processor's delivery of the Services to the Data Controller the Data Processor will process certain categories and types of the Data Controller's personal data on behalf of the Data Controller.

3.3 "Personal data" includes "*any information relating to an identified or identifiable natural person*" as defined in GDPR, article 4 (1) (1) (the "Personal Data"). The categories and types of Personal Data processed by the Data Processor on behalf of the Data Controller are listed in Appendix A. The Data Processor only performs processing activities that are necessary and relevant to perform the Services. The parties shall update Appendix A whenever changes occur that necessitates an update.

3.4 The Data Processor shall have and maintain a register of processing activities in accordance with GDPR, article 32 (2).

4. Instruction

4.1 The Data Processor may only act and process the Personal Data in accordance with the documented instruction from the Data Controller (the "Instruction"), unless required by law to act without such instruction. The Instruction at the time of entering into this Agreement is that the Data Processor may only process the Personal Data with the purpose of delivering the Services. Subject to the terms of this DPA and with mutual agreement of the parties, the Data Controller may issue additional written instructions consistent with the terms of this Agreement. The Data Controller is responsible for ensuring that all individuals who provide written instructions are authorised to do so.

4.2 The Data Controller guarantees to process Personal Data in accordance with the requirements of applicable Data Protection Laws and Regulations. The Data Controller's instructions for the processing of Personal Data shall comply with applicable Irish and European law. The Data Controller will have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which it was obtained.

4.3 The Data Processor will inform the Data Controller of any instruction that it deems to be in violation of applicable law and will not execute the instructions until they have been confirmed or modified.

5. Confidentiality

5.1 Confidentiality

5.1.1 The parties agree that "**Confidential Information**" means (a) all patient Personal Data exchanged between the parties as part of the carrying out the Services; and shall mean (b) any other data or information designated in writing by one Party to the other Party to be confidential or relating to Services or any survey, activities or business of the other Party.

5.1.2 In consideration of a disclosing Party making Confidential Information available to a recipient Party, the recipient Party agrees that it will:

(a) take all actions necessary to keep confidential the Confidential Information;
(b) not disclose the Confidential Information supplied to any third party, corporation or other person whatsoever without the written consent of the disclosing Party;
(c) not copy, disseminate or use such Confidential Information except as expressly authorised in writing by the disclosing Party.

5.1.3 The Parties agree that the obligations of confidentiality shall not apply to that part of the Confidential Information which:

- at the time of disclosure is information already generally available to the public;
- is independently received from a third party having a *bona fide* right to use or disclose it;
- the recipient Party can demonstrate by written record was developed by the recipient Party independently of the disclosure of Confidential Information by the disclosing Party.

5.1.4 If either Party is required to disclose all or part of the Confidential Information by any law, governmental or regulatory authority, supervisory body or authority of competent jurisdiction to whose rules a Party is subject, it will be entitled to do so, provided in each case that a Party shall immediately consult with the other Party in advance as to the form, content and timing of the disclosure and shall take all reasonable action to limit such disclosure.

5.1.5 The Data Processor's employees shall be subject to an obligation of confidentiality that ensures that the employees shall treat all the Personal Data under this Agreement with strict confidentiality.

5.1.6 Personal Data will only be made available to personnel that require access to such Personal Data for the delivery of the Services and this Agreement.

5.1.7 The Data Processor shall also ensure that employees processing the Personal Data only process the Personal Data in accordance with the Instructions of the Data Controller.

5.1.8 The Data Processor shall not retain any copy of Data Controller Personal Data whatsoever following completion of the term of the Services.

5.2 Security

5.2.1 The Data Processor shall implement and keep in place the appropriate technical and organizational measures as set out in this Agreement and in the applicable law, including in accordance with GDPR, Article 32. The Data Processor may update or modify the security measures from time-to-time provided that such updates and modifications do not result in the degradation of the overall security and meet the requirements of Article 32 of GDPR.

5.3 The Data Processor shall provide documentation for the Data Processor's security measures if requested by the Data Controller in writing.

5.4 Data protection impact assessments and prior consultation

5.4.1 If the Data Processor's assistance is necessary and relevant, the Data Processor shall assist the Data Controller in preparing data protection impact assessments in accordance with GDPR, article 35, along with any prior consultation in accordance with GDPR, article 36.

5.5 Rights of the data subjects

5.5.1 If the Data Controller receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and the correct and legitimate reply to such a request necessitates the Data Processor's assistance, the Data Processor shall assist the Data Controller by providing the necessary information and documentation. The Data Processor shall be given reasonable time to assist the Data Controller with such requests in accordance with the Applicable Law.

5.5.2 If the Data Processor receives a request from a data subject for the exercise of the data subject's rights under the Applicable Law and such request is related to the Personal Data of the Data Controller, the Data Processor must immediately forward the request to the Data Controller and must refrain from responding to the person directly.

5.6 Personal Data Breaches

5.6.1 The Data Processor shall give immediate notice to the Data Controller if a breach occurs, that can lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to, personal data transmitted, stored or otherwise processed re the Personal Data processed on behalf of the Data Controller (a "Personal Data Breach").

5.6.2 The Data Processor shall make reasonable efforts to identify the cause of such a breach and take those steps as they deem necessary to establish the cause, and to prevent such a breach from reoccurring.

5.7 Documentation of compliance and Audit Rights

5.7.1 Upon request by a Data Controller, the Data Processor shall make available to the Data Controller all relevant information necessary to demonstrate compliance with this DPA, and shall allow for and reasonably cooperate with audits, including inspections by the Data Controller or an auditor mandated by the Data Controller. The Data Controller shall give notice of any audit or document inspection to be conducted and shall make reasonable endeavours to avoid causing damage or disruption to the Data Processors premises, equipment and business in the course of such an audit or inspection. Any audit or document inspection shall be carried out with reasonable prior written notice of no less than 30 days, and shall not be conducted more than once a year.

5.7.2 The Data Controller may be requested to sign a non-disclosure agreement reasonably acceptable to the Data Processor before being furnished with the above.

6. Sub-Processors

6.1 The Data Processor can only engage third-parties to process the Personal Data ("Sub-Processors") with receipt of written, specific authorization from the Data Controller.

6.2 The Data Processor shall (if authorised) complete a written sub-processor agreement with any Sub-Processors. Such an agreement shall at minimum provide the same data protection obligations as the ones applicable to the Data Processor, including the obligations under this Agreement. The Data Processor shall on an ongoing basis monitor and control its Sub- Processors' compliance with the Applicable Law. Documentation of such monitoring and control shall be provided to the Data Controller if so requested in writing.

6.3 The Data Processor is accountable to the Data Controller for any Sub-Processor in the same way as for its own actions and omissions.

7. Duration

7.1 This Agreement shall remain in force unless it is terminated in writing on 60 days' notice to the other party however the obligations with regard to confidentiality will survive for a period of 4 years post any termination.

8. Data Protection Officer

8.1 The Data Processor contact for this agreement is: Peter Feeney, DPO, NUI Galway

8.2 The Data Controller contact for this Agreement is: Liam Quirke, DDPO, HSE West.

9. Termination

9.1 Following expiration or termination of the Agreement, the Data Processor will delete or return to the Data Controller all Personal Data in its possession as provided in the Agreement except to the extent the Data Processor is required by Applicable law to retain some or all of the Personal Data (in which case the Data Processor will archive the data and implement reasonable measures to prevent the Personal Data from any further processing). The terms of this DPA will continue to apply to such Personal Data.

Agreement

We agree to the terms of this Agreement

30.07.2020

(On behalf of HSE) Date
Professor Michael Kerin,
Director Saolta Cancer Managed & Clinical Academic Network

30.07.2020

(On behalf NUIG) Date
Professor Tim O'Brien,
Dean of School of Medicine,
NUI Galway

Appendix A

1. Personal Data

The Data Processor processes the following types of Personal Data in connection with its delivery of the Services:

1. Information on relevant biobank participants from the Data Controller relevant for the processing and compiling the Cancer, Managed Clinical & Academic Network (CMCAN) Biobank Database and associated datasets. Namely: biological samples like tissue, blood, saliva, buccal swabs, urine; AND some limited personal details and clinical information are also required, for example: name, date of birth, address, board number, hospital number and Consultant Surgeon. Also special category personal health and genetic data, such as: risk factors, lifestyle data, prophylactic, diagnostic, therapeutic procedures and reconstructive procedures, histology, disease staging, prognostic indices, genetic test results, family history of cancer, treatment, disease progression, and survival data.

   2. Categories of data subjects

2.1 The Data Processor processes personal data about the following categories of data subjects on behalf of the Data Controller:

1. Cancer Patients
2. Health Research Control Patients
3. Healthy Volunteers