ST ANDREW'S HEALTHCARE
DATA PROCESSING AGREEMENT

PARTIES

CHARITY	ST ANDREW'S HEALTHCARE (COMPANY NUMBER 5176998) BILLING ROAD, NORTHAMPTON, NN1 5DG	
SUPPLIER	**NAME**	
	COMPANY NUMBER	
	ADDRESS	

BACKGROUND

The Parties have entered into the Main Contract under which the Charity will provide data to the Supplier for processing which is covered by the Data Protection Laws. The parties have agreed to enter into this Agreement in order to confirm the terms which will regulate the parties' obligations in relation to such data.

DEFINITIONS AND INTERPRETATIONS

1.1 In this Agreement:

Applicable Law means:

(a) any law, statute, regulation, byelaw or subordinate legislation in force from time to time to which a party is subject and/or in any jurisdiction that the Services are provided to or in respect of;

(b) the common law and laws of equity as applicable to the parties from time to time;

(c) any binding court order, judgment or decree;

(d) any applicable industry code, policy or standard; or

(e) any applicable direction, policy, rule or order that is binding on a party and that is made or given by any regulatory body having jurisdiction over a party or any of that party's assets, resources or business;

Business Day means a day other than a Saturday, Sunday or bank or public holiday in England;

Charity Policies the Charity's business policies, procedures, rules and codes as advised, or made available, to the Supplier from time to time;

Complaint means a complaint or request relating to either party's obligations under Data Protection Laws relevant to this Agreement, including any compensation claim from a Data Subject or any notice, investigation or other action from a Supervisory Authority;

Data Controller has the meaning given to that term (or to the term 'controller') in Data Protection Laws;

Data Processor has the meaning given to that term (or to the term 'processor') in Data Protection Laws;

Data Protection Laws means any Applicable Law relating to the processing, privacy, and use of Personal Data, as applicable to the Charity, the Supplier and/or the Services, including:

(a) the Data Protection Act 1998 and the Privacy and Electronic Communications (EC

Directive) Regulations 2003, SI 2003/2426, and any laws or regulations implementing Directive 95/46/EC (**Data Protection Directive**) or Directive 2002/58/EC (**ePrivacy Directive**); and/or

(b) the General Data Protection Regulation (EU) 2016/679 (**GDPR**), and/or any corresponding or equivalent national laws or regulations (**Revised UK DP Law**); and

(c) any judicial or administrative interpretation of any of the above, any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant Supervisory Authority;

Data Protection Losses means all liabilities and other amounts, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage);

(b) loss or damage to reputation, brand or goodwill;

(c) to the extent permitted by Applicable Law:

(i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority;

(ii) compensation paid to a Data Subject (including compensation to protect goodwill and ex gratia payments); and

(iii) costs of compliance with investigations by a Supervisory Authority; and

(d) the costs of loading Charity data, to the extent the same are lost, damaged or destroyed, and any loss or corruption of Charity data (including the costs of rectification or restoration of Charity data);

Data Subject has the meaning given to that term in Data Protection Laws;

Data Subject Request means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws;

International Organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

International Recipient has the meaning given to that term in clause 7;

Main Contract means the contract(s) between the Parties for the provision of good and/or services to the Charity;

Personal Data has the meaning given to that term in Data Protection Laws;

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

processing has the meanings given to that term in Data Protection Laws (and related terms such as **process** have corresponding meanings);

Processing Instructions has the meaning given to that term in clause 3.1.1;

Protected Data means Personal Data received from or on behalf of the Charity, or otherwise obtained in connection with the performance of the Supplier's obligations under the Main Contract

and this Agreement;

Services	means any goods and/or services provided pursuant to the Main Contract; and
Supervisory Authority	means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws.

1.2. References to legislation are a reference to that legislation as amended, extended, enacted or re-enacted and references to terms defined in such legislation shall include the equivalent terms defined in such legislation. A reference to a law includes all subordinate legislation made under that law; and

1.3 This Agreement shall survive termination (for any reason) or expiry of the Main Contract (or of any of the Services).

DATA PROCESSING PROVISIONS

2 Data Processor and Data Controller

2.1 The parties agree that, for the Protected Data, the Charity shall be the Data Controller and the Supplier shall be the Data Processor.

2.2 The Supplier shall comply with all Data Protection Laws in connection with the processing of Protected Data, the Services and the exercise and performance of its respective rights and obligations under the Main Contract and this Agreement and shall not, by any act or omission, cause the Charity (or any other person) to be in breach of any Data Protection Laws.

2.3 The Charity shall comply with all Data Protection Laws in respect of the performance of its obligations under the Main Contract and this Agreement.

3 Instructions and details of processing

3.1 Insofar as the Supplier processes Protected Data on behalf of the Charity, the Supplier:

3.1.1 unless required to do otherwise by Applicable Law, shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Charity's documented instructions as set out in this clause 3 and the Schedule (Data Processing Details), and as updated from time to time by the written agreement of the parties (**Processing Instructions**); and

3.1.2 if Applicable Law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Charity of any such requirement before processing the Protected Data (unless Applicable Law prohibits such on important grounds of public interest).

3.2 The Supplier shall immediately inform the Charity in writing if, in the Supplier's opinion, a Processing Instruction infringes the Data Protection Laws or any other Applicable Laws relating to data protection and explain the reasons for its opinion, provided that this shall be without prejudice to clause 2.2.

3.3 The processing to be carried out by the Supplier under this Agreement shall comprise the processing set out in the Schedule (Data Processing Details), and such other processing as agreed by the parties in writing from time to time.

4 Technical and organisational measures

4.1 The Supplier shall implement and maintain, at its cost and expense, appropriate technical and organisational measures in relation to the processing of Protected Data by the Supplier:

4.1.1 such that the processing will meet the requirements of Data Protection Laws and ensure the protection of the rights of Data Subjects;

4.1.2 so as to ensure a level of security in respect of Protected Data processed by it that is appropriate to the risks that are presented by the processing, in particular from accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed; and

4.1.3 without prejudice to clause 6.1, insofar as is possible, to assist the Charity in the fulfilment of the Charity's obligations to respond to Data Subject Requests relating to Protected Data.

4.2 Without prejudice to clause 4.1, the Supplier shall, in respect of the Protected Data processed by it under this Agreement comply with the requirements regarding security of processing set out in Data Protection Laws (as applicable to Data Processors), all relevant Charity Policies and this Agreement.

5 Using staff and other processors

5.1 The Supplier shall not engage another Data Processor (or any replacement) for carrying out any processing activities in respect of the Protected Data without the Charity's specific prior written consent.

5.2 The Supplier shall ensure that the Supplier personnel and all other persons authorised by it , or by any person acting on its behalf (including by any Data Processor pursuant to clause 5.1), to process Protected Data are subject to a binding written contractual obligation with the Supplier (or with the Data Processor that has engaged them) to keep the Protected Data confidential (except where disclosure is required in accordance with Applicable Law, in which case the Supplier shall, where practicable and not prohibited by Applicable Law, notify the Charity of any such requirement before such disclosure).

5.3 Without prejudice to any other provision of this Agreement, the Supplier shall ensure that the Supplier personnel processing Protected Data are reliable and have received adequate training on compliance with this Agreement and the Data Protection Laws applicable to the processing.

5.4 The Supplier shall ensure that access to Protected Data is limited to the authorised persons who need access to it to supply the Services.

6 Assistance with the Charity's compliance and Data Subject rights

6.1 The Supplier shall (at no cost to the Charity):

6.1.1 record and then refer all Data Subject Requests it receives to the Charity within two Business Days of receipt of the request;

6.1.2 provide such information and cooperation and take such action as the Charity reasonably requests in relation to each Data Subject Request, within the timescales reasonably required by the Charity; and

6.1.3 not respond to any Data Subject Request or Complaint without the Charity's prior written approval.

6.2 Without prejudice to clause 3.1, the Supplier shall, at its cost and expense, provide such information, co-operation and other assistance to the Charity as the Charity reasonably requires (taking into account the nature of processing and the information available to the Supplier) to ensure compliance with the Charity's obligations under Data Protection Laws, including with respect to:

6.2.1 security of processing;

6.2.2 data protection impact assessments (as such term is defined in Data Protection Laws);

6.2.3 prior consultation with a Supervisory Authority regarding high risk processing; and

6.2.4 any remedial action and/or notifications to be taken in response to any Personal Data Breach and/or Complaint, including (subject in each case to the Charity's prior written authorisation) regarding any notification of the Personal Data Breach to Supervisory Authorities and/or communication to any affected Data Subjects.

7 International data transfers

The Supplier shall not transfer any Protected Data to any country outside the European Economic Area or to any International Organisation (an **International Recipient**) without the Charity's prior written consent.

8 Records, information and audit

8.1 The Supplier shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of the Charity, containing such information as the Charity may reasonably require, including:

8.1.1 the name and contact details of the Data Processor(s) and of each Data Controller on behalf of which the Data Processor is acting, and of the Supplier's representative and data protection officer (if any);

8.1.2 the categories of processing carried out on behalf of each Data Controller;

8.1.3 where applicable, details of transfers of Protected Data to an International Recipient; and

8.1.4 a general description of the technical and organisational security measures referred to in clause 4.1.

8.2 The Supplier shall make available to the Charity on request in a timely manner (and in any event within three Business Days):

8.2.1 copies of the records under clause 8.1; and

8.2.2 such other information as the Charity reasonably requires to demonstrate the Supplier's and the Charity's compliance with their respective obligations under Data Protection Laws and this Agreement.

8.3 The Supplier shall at no cost to the Charity:

8.3.1 allow for and contribute to audits, including inspections, conducted by the Charity or another auditor mandated by the Charity for the purpose of demonstrating compliance by the Supplier and the Charity with their respective obligations under Data Protection Laws and this Agreement; and

8.3.2 provide (and procure) reasonable access for the Charity or such other auditor (where practicable, during normal business hours) to:

8.3.2.1 the facilities, equipment, premises and sites on which Protected Data and/or the records referred to in clause 8.1 are held, and to any other equipment or facilities used in the provision of the Services (in each case whether or not owned or controlled by the Supplier); and

8.3.2.2 to the relevant Supplier's personnel,

provided that the Charity gives the Supplier reasonable prior notice of such audit and/or inspection.

8.4 If any audit or inspection reveals a material non-compliance by the Supplier with its obligations under Data Protection Laws or a breach by the Supplier under this Agreement, the Supplier shall pay the reasonable costs of the Charity or its mandated auditors, of the audit or inspection.

8.5 The Supplier shall promptly resolve, at its own cost and expense, all data protection and security issues discovered by the Charity and reported to the Supplier that reveal a breach or potential breach by the Supplier of its obligations under this Agreement.

8.6 If the Supplier is in breach of its obligations under this Agreement, the Charity may (without being in breach of the Main Contract) suspend the transfer of Protected Data to the Supplier until the breach is remedied.

8.7 The Charity shall be entitled to share any notification, details, records or information provided by or on behalf of the Supplier under this Agreement (including under clauses 8 or 9) with any other company within the Charity's group, its professional advisors and/or the Supervisory Authority.

9 Breach notification

9.1 In respect of any Personal Data Breach, the Supplier shall:

9.1.1 notify the Charity of the Personal Data Breach without undue delay (but in no event later than 12 hours after becoming aware of the Personal Data Breach); and

9.1.2 provide the Charity without undue delay (wherever possible, no later than 24 hours after becoming aware of the Personal Data Breach) with such details as the Charity reasonably requires regarding:

9.1.2.1 the nature of the Personal Data Breach, including the categories and approximate numbers of Data Subjects and Protected Data records concerned;

9.1.2.2 any investigations into such Personal Data Breach;

9.1.2.3 the likely consequences of the Personal Data Breach; and

9.1.2.4 any measures taken, or that the Supplier recommends, to address the Personal Data Breach, including to mitigate its possible adverse effects,

provided that, (without prejudice to the above obligations) if the Supplier cannot provide all these details within the timeframes set out in this clause 9.1.2, it shall (before the end of such timeframes) provide the Charity with reasons for the delay and when it expects to be able to provide the relevant details (which may be phased), and give the Charity regular updates on these matters.

9.2 The Supplier shall promptly (and in any event within two Business Days) inform the Charity if it receives a Complaint and provide the Charity with full details of such Complaint.

10 Deletion or return of Protected Data and copies

The Supplier shall (and shall ensure that all persons acting on its behalf and all Supplier personnel shall) without delay (and in any event within two Business Days), either securely delete or (at the Charity's option) securely return all the Protected Data to the Charity in such form as the Charity reasonably requests after the earlier of:

10.1 the end of the provision of the relevant Services related to processing of such Protected Data; or

10.2 once processing by the Supplier of any Protected Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under this Agreement,

and securely delete existing copies (unless storage of any data is required by Applicable Law and, if so, the Supplier shall inform the Charity of any such requirement).

11 Liability and indemnities

11.1 The Supplier shall indemnify and keep indemnified the Charity in respect of all Data Protection Losses suffered or incurred by, awarded against or agreed to be paid by, the Charity or any member of the Charity Group arising from or in connection with:

11.1.1 any breach by the Supplier of any of its obligations under this Agreement; or

11.1.2 the Supplier (or any person acting on its behalf) acting outside or contrary to the lawful Processing Instructions of the Charity in respect of the processing of Protected Data.

11.2 This clause 11 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:

11.2.1 to the extent not permitted by Applicable Law (including Data Protection Laws); and

11.2.2 that it does not affect the liability of either party to any Data Subject.

12 General

12.1 The Supplier may not assign or subcontract all or any of its rights or obligations under this Agreement without the prior written consent of the Charity.

12.2 Any notices shall be in writing, addressed to that party at its registered office (if it is a company) or its principal place of business (in any other case) and shall be delivered personally, or sent by pre-paid first class post or other next working day delivery service, commercial courier.

12.3 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such

modification is not possible, the relevant provision or part-provision shall be deleted. The remainder of this Agreement shall be unaffected.

12.4 A waiver of any right or remedy under this Agreement or law is only effective if given in writing. No failure or delay by a party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy.

12.5 Nothing in this Agreement is intended to establish any partnership or joint venture or agency between the parties.

12.6 A person who is not a party to this Agreement shall not have any rights to enforce its terms.

12.7 No variation of this Agreement shall be effective unless it is in writing and signed by the Charity.

12.8 This Agreement, and any dispute or claim arising out of shall be governed by, and construed in accordance with the law of England and Wales and shall be subject to the exclusive jurisdiction the courts of England and Wales.

This Agreement has been entered into on the date last stated below:

	Signed by the Charity	**Signed by the Supplier**
Signature		
Name		
Position	Director	Director
Date		

THE SCHEDULE
DATA PROCESSING DETAILS

1 Subject-matter of processing

[This should be a high level, short description of what the processing is about i.e. its subject matter. An example would be processing of employees' personal data in the specific employment context, or processing of patient data for health related purposes]

2 Duration of the processing

[Clearly set out the duration of the processing including dates for the start and end of the processing]

3 Nature and purpose of the processing

[The term "processing" is very broad. It essentially means anything that is done to, or with, personal data. In order to process personal data, the Charity needs to identify a lawful basis as set out in the General Data Protection Regulation. One or more lawful basis from Article 6 is required for all personal data. One or more lawful basis for processing from Article 9 for special categories personal data. "Processing" then means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. The purpose might include: employment processing, statutory obligation, recruitment assessment etc.]

4 Type of Personal Data

[The personal data processed may concern the following details such as a Natural Person's name, date of birth, gender, address, email address, telephone number, Patient RiO number, employee ID, employment and pensionable service status and periods, dates of absence, employment grade, employee performance, job title, salary and remuneration arrangements, pension amounts, pension contributions, employee benefit details, insurance cover, marital status, beneficiary details, bank details, national insurance number/national identification number/social security number, underwriting status, business travel information, educational background, passport number, driving licence number, psychometric test results]

5 Special Categories of Personal Data

[The personal data processed may concern the following special categories of data: Details of a Natural Person's health, race, ethnic origin, genetics, biometrics (where used for ID purposes), sex life, sexual orientation, trade union membership, political affiliation]

6 Categories of Data Subject

[This is the term used to describe individuals about which personal data is held. The Personal Data Processed may concern the following categories of Natural Person's: patients family, associates and representatives of the person whose personal data we are processing, customers and clients, staff, suppliers, business contacts, professional advisers and consultants, visitors, complainants, correspondents and enquirers, members or supporters, offenders and suspected offenders]

7 Processing Instructions

Without prejudice to its other obligations, the Supplier shall implement and maintain at least the following technical and organisational security measures to protect the Protected Data:

1. In accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with this Agreement, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, the

Supplier shall implement appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the GDPR.

2. Without prejudice to its other obligations, the Supplier shall comply with the Charity's Data Protection and Information Security Policies and procedures and any necessary additional controls based on the nature of the engagement, or service procured. Depending on the nature of the services, the Charity may ask for evidence of the following items (which the Supplier agrees to provide):

- Evidence of information security and data protection policies
- Evidence of information security and data protection procedures for example, a procedure for handling Subject Access Requests and other rights of the individual, a procedure for Data Breach Management, a procedure for access management
- Record of activities and assets processed on behalf of the Charity
- Evidence of the undertaking of mandatory information security and data protection training of staff
- Evidence of data processing contracts, which are compliant with requirement of Article 28 of GDPR, with all approved sub-processors.
- Evidence that the Supplier has assured the compliance of all their approved sub-processors.