Data Processing Agreement

Between

<<Practice>>

And

Delt Shared Services Ltd

Date Effective from <<Today>>

Version: 1.0

2 DATA PROTECTION PROTOCOL

1 Table A – Processing, Personal Data and Data Subjects

Description	Details
Subject matter of the Processing	Any and all data held in or temporarily generated by the clinical systems supported by the GPintheCloud service as part of the operation of the clinical system.
Duration of the Processing	This agreement will commence on <<Today>> and be in place for the duration of the service. The processing is not occasional.
Nature and purposes of the Processing	The purpose of the processing is solely to provide the mechanism over which supported clinical systems can be viewed remotely by persons authorised and controlled by the respective data controller. Delt Shared Servies Ltd. will have no access to the clinical system data, which remains under the control of its respective data controller. Depending on the operation of a clinical system for which the data controller has provided access, temporary files may be generated in the virtual machine. Delt Shared Services Ltd will not access or attempt to access this data, unless instructed by the Practice.
Type of Personal Data	The following data will be viewed via GPintheCloud for Locums to provide direct care to the practice's registered patients direct: ● Name ● Address ● Data of birth ● NHS number ● Healthcare information (as documented in the clinical record) ● Family, lifestyle and social circumstances ● Religious or other beliefs of a similar nature ● Physical or mental health conditions ● Information relating to sexual health or orientation The following data will be pulled from the Clinical System regarding employees (who have entered into the patient's record): ● Name ● Job Title

Categories of Data Subject	Patient data – this will be specifically for patients registered with the practice who are being seen by the Locum via GPintheCloud. Employee's data – All employees who work within the practice and contribute to the practice's clinical system. This could be employees who work for the practice permanently (such as Clinicians or Administrators) or on an ad hoc basis (such as Locums).
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data	Any temporary files generated by the clinical data system that the clinical data system does not also dispose of will be deleted at the end of the virtual machines lifespan (not more than 30 days).

3 Definitions

"**Data Loss Event**"	means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach**;**
"**Data Protection Impact Assessment**"	means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data;
"**Data Protection Officer**" and **"Data Subject**"	shall have the same meanings as set out in the GDPR;
"**Data Subject Access Request**"	means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.
"**Personal Data Breach**"	shall have the same meaning as set out in the GDPR;
"**Protective Measures**"	means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it;
"**Protocol**" or "**Data Protection Protocol**"	means this Data Protection Protocol;
"**Sub-processor**"	means any third party appointed to Process Personal Data on behalf of the Supplier related to this Contract.

1 DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the GP Practice ["the Authority"] is the Controller and Delt Shared Services Ltd ["the Supplier"] is the Processor. The only Processing that the Supplier is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier.

1.2 The Supplier shall notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.

1.3 The Supplier shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Authority, include:

1.3.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;

1.3.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Services;

1.3.3 an assessment of the risks to the rights and freedoms of Data Subjects; and

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

1.4 The Supplier shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:

1.4.1 process that Personal Data only in accordance with Table A of this Protocol, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Authority before Processing the Personal Data unless prohibited by Law;

1.4.2 ensure that it has in place Protective Measures, which have been reviewed and approved by the Authority as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

1.4.3 ensure that :

(i) the Supplier Personnel do not Process Personal Data except in accordance with this Contract (and in particular Table A of this Protocol);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Supplier's duties under this Protocol;

(B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority or as otherwise permitted by this Contract; and

(D) have undergone adequate training in the use, care, protection and handling of Personal Data;

1.4.4 not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:

(i) the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the GDPR or Article 37 of the Law Enforcement Directive (Directive (EU) 2016/680)) as determined by the Authority;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Supplier complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Authority in meeting its obligations); and

(iv) the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data;

1.4.5 at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination or expiry of the Contract unless the Supplier is required by Law to retain the Personal Data.

1.5 Subject to Clause 1.6 of this Protocol, the Supplier shall notify the Authority immediately if it:

1.5.1 receives a Data Subject Access (or purported Data Subject Access Request), Freedom of Information or Environmental Information Regulation (EIR) request;

1.5.2 receives a request to rectify, block or erase any Personal Data;

1.5.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

1.5.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Contract;

1.5.5 receives a request from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

1.5.6 becomes aware of a Data Loss Event.

1.6 The Supplier’s obligation to notify under Clause 1.5 of this Protocol shall include the provision of further information to the Authority in phases, as details become available.

1.7 Taking into account the nature of the Processing, the Supplier shall provide the Authority with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 of this Protocol (and insofar as

possible within the timescales reasonably required by the Authority) including by promptly providing:

1.7.1 the Authority with full details and copies of the complaint, communication or request;

1.7.2 such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

1.7.3 the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;

1.7.4 assistance as requested by the Authority following any Data Loss Event;

1.7.5 assistance as requested by the Authority with respect to any request from the Information Commissioner's Office, or any consultation by the Authority with the Information Commissioner's Office.

1.8 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Protocol. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

1.8.1 the Authority determines that the Processing is not occasional;

1.8.2 the Authority determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

1.8.3 the Authority determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.9 The Supplier shall allow for audits of its Processing activity by the Authority or the Authority's designated auditor.

1.10 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.11 Before allowing any Sub-processor to Process any Personal Data related to this Contract, the Supplier must:

1.11.1 notify the Authority in writing of the intended Sub-processor and Processing;

1.11.2 obtain the written consent of the Authority;

1.11.3 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Protocol such that they apply to the Sub-processor; and

1.11.4 provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.

1.12 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

1.13 The Authority may, at any time on not less than 30 Business Days' notice, revise this Protocol by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).

1.14 The Parties agree to be compliant with any guidance issued by the Information Commissioner's Office. The Authority may on not less than 30 Business Days' notice to the Supplier amend this Protocol to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.15 The Supplier shall comply with any further instructions with respect to Processing issued by the Authority by written notice. Any such further written instructions shall be deemed to be incorporated into Table A above from the date at which such notice is treated as having been received by the Supplier.

1.16 Subject to Clauses 1.13, 1.14, and 1.15 of this Protocol, any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

1.17 The information processing and this agreement will be reviewed by a suitably qualified individual or committee/group by the Controller and Supplier, at a minimum annually, and on an ad hoc basis as and when required to ensure the agreement remains fit for purpose and that the information processing is continuing to effectively achieve its objectives. This agreement will remain in force irrespective of whether the agreement has been officially reviewed until a notice of termination is served.

Signed for and on behalf of: Delt Shared Services Ltd.	
Name:	Giles Letheren
Position:	CEO
Signature:	Giles Letheren <<Today>>
Date:	<<Today>>

Signed for and on behalf of <<Practice>>	
Name:	<<First name>> <<Last name>>
Position:	<<Your position>>
Signature:	**<<First name>> <<Last name>>** - NHS email <<NHS email>>
Date:	<<Today>>