Data Processing Agreement

1 DATA PROTECTION

1.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the identity of the Controller and the `Processor for each category of Personal Data is as set out in Table A below.

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 Services:

1.4.1 process that Personal Data only in accordance with Table A, 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 does not Process Personal Data except in accordance with any relevant contractual commitment.

(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 Data Processing Agreement;

(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(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Authority or as otherwise permitted by any relevant 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 UK or the EU unless Supplier has previously notified the Authority 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 UK 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 (by means of an adequacy decision) 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 any relevant contract unless the Supplier is required by Law to retain the Personal Data and provide a certificate of destruction.

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 Request (or purported Data Subject Access 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 Data Processing Agreement 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 to comply with Article 30 UK GDPR

'Records of processing activities'. 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 UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK 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 enter into a written agreement with the Sub-processor which give effect to the terms set out in this Data Processing Agreement such that they apply to the Sub-processor; and

1.11.3 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 Supplier may, at any time on not less than 30 Business Days' notice, revise this Data Processing Agreement 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 any relevant contract with the Authority).

1.14 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Authority may on not less than 30 Business Days' notice to the Supplier ask the Supplier to amend this Data Processing Agreement 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 when incorporated into any relevant contract between the Supplier and the Authority.

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 DATA PROTECTION PROTOCOL (UK GDPR Article 28(3))

1 Table A – Processing, Personal Data and Data Subjects

Description	Details
Identity of Controller and Processor for each Category of Personal Data	The Authority is Controller and the Supplier is Processor of all patient data. The Parties are Independent Controllers of Personal Data in respect of; • Business contact details of Supplier Personnel for which the Supplier is the Controller, • Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under the Contract and/or Agreement) for which the Buyer is the Controller, • All analytical data including Identity Data, Contact Data, Technical data, Preference Data, Marketing and Communications Data and Usage data (as defined in our Privacy Notice) of all users of the Pando App aggregated to measure effectiveness of our products and services and to provide improvements to the products and services and to manage the contractual relationship between the parties. • Pseudonymised messages posted on the Pando App • Subject to compliance with the National opt out pseudonymised patient data to help improve patient outcomes and offer improvements to the products and services.
Duration of the processing	Up to 8 years after the expiry or termination of any relevant contract between the Authority and the Supplier.

Nature and purposes of the processing	The Supplier will process Personal Data on behalf of the Authority To facilitate the fulfilment of the Supplier's obligations arising under any relevant Agreement including; i. Ensuring effective communication between the Supplier and the Authority ii. Maintaining full and accurate records of every Contract and/or Agreement arising between the Parties. iii – measuring the effectiveness of the products and services and to enable development thereof for improved patient outcomes The nature of the Processing means any operation 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 of data (whether or not by automated means) etc. The Supplier will process Personal Data on behalf of the Authority for the purposes as detailed below: ● To deliver person centred health and/or care ● To fulfil contractual obligations ● To satisfy Audit / Regulatory requirements and inspections
Type of Personal Data	Patient: 1. Name 2. Address (home or business) 3. Postcode 4. NHS No 5. Ethnic origin may be captured 6. Sexual orientation may be captured 7. Race may be captured 8. Sex life may be captured 9. Religion of philosophical belief may be captured. 10. Date of birth 11. Images

	12. Details about medical conditions/health User: Healthcare Professional 13. IP address 14. Login data including biometrics. 15. Clinical specialty/care setting 16. Role 17. Bio 18. Notes 19. Special interests 20. Place of work 21. Email address 22. Phone 23. Ask Advice Teams 24. Faculty/Affiliation 25. GMC number 26. Optional Profile Picture
Categories of Data Subject	Includes: i. Contact details of, and communications with, Authority staff concerned with management of the Contract and/Agreement ii. Contact details of, and communications with, Supplier staff concerned with award and management of the Contract and/or Agreement with the Authority, iii. Contact details, and communications with, Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from the Contract and/or Agreement iv Contact details, and communications with Supplier staff concerned with management of the Contract and/or Agreement v-Contact details and communications with clinical staff and patients engaged in provision of the Services supplied by the Supplier
Categories of Data Subject/International transfers and legal gateway	Includes: i. Authority staff concerned with management of the Contract and/or Agreement ii. Supplier staff concerned with award and management of Contract and/or Agreement

	iii. Sub-contractor staff concerned with fulfilment of the Supplier's obligations arising from the Contract and/or Agreement iv. Supplier staff concerned with fulfilment of the Supplier's obligations arising under the Contract and/or Agreement v. Patients whose data is provided during the course of provision of the Services under the Contract and/or Agreement
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	All relevant data to be deleted 8 years after the expiry or termination of the Contract and/or Agreement unless longer retention is required by Law or the terms of any Contract and/or Agreement

2 Definitions

The definitions and interpretative provisions at Schedule 4 (Definitions and Interpretations) of the Contract and/or Agreement shall also apply to this Protocol. Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

"Authority"	means the relevant authority (including the Crown Commercial Services) whom have entered into a contract with the Supplier.
"Contract and/or Agreement"	means the Contract or Agreement between the relevant Authority and the Supplier, including any Agreement, Framework Agreement, Call Off Contract or other Contract.
"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 Agreement, 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 UK 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 UK 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;
"Sub-processor"	means any third party appointed to Process Personal Data on behalf of the Supplier related to this Contract and/or Agreement.

Wet Signatures are not required on the condition that the parties provide an unequivocal approval of terms email from the authorised signatory which will be appended to the final agreement.

Name	
Role	
Signature / Email Attached	
Date	
Trust Caldicott Guardian / Chief Clinical Information Officer	
Name	Frank Seo
Role	CEO
Signature / Email Attached	
Date	
Data Processor Signatory	
Name	Philip Mundy
Role	Founder and co-CEO
Signature / Email Attached	
Date	