Pando
DATA PROCESSING AGREEMENT

PARTIES

(1) FORWARD CLINICAL LTD incorporated and registered in England and Wales with company number 10420044 whose registered office is at:

300 St John Street, London, EC1V 4PA United Kingdom (Supplier) and who is registered with the ICO under number ZA237861.

(2) TRUST/HEALTHCARE/GOVERNMENT/COUNCIL/ ORGANISATION: [PARTNER NAME]

SECTION A - AGREEMENT AND KEY DETAILS

(A) The Supplier has developed a secure mobile communications and workflow application for healthcare and service professionals known as 'Pando'.

(B) The Supplier provides Pando as an application that is installed on an end-user's mobile device and software that is provided as a service and runs under the control of the Supplier on remote servers.

(C) The Supplier provides various additional services such as implementation, training and consulting services in support of its software application.

(D) The Partner wishes to use the Supplier's software and services in its organisation and the Supplier has agreed to provide the software and services.

This Agreement comprises:

- Section A - Agreement and Key Details, including this cover page and the signature clauses;
- Section B - General Terms and Definitions;
- Section C – Data Processing Agreement

SECTION A - AGREEMENT AND KEY DETAILS

Software: Pando – a secure mobile communications and workflow application for healthcare and service professionals.

Installed Environment: Hospital / Trust / Practice/Council

Start Date: _____

Partner Project Manager: _____

SIGNED

Signed by Philip Mundy (Director)

for and on behalf of FORWARD CLINICAL LTD

_____

Authorised Signatory

Signed by

_____

for and on behalf of the Partner Organisation

_____

Authorised Signatory

SECTION B - GENERAL TERMS AND DEFINITIONS

Acceptable Use Policy: The policy issued by Supplier from time to time concerning use of the Pando Application in accordance with good practice and public sector standards. The Acceptable Use Policy can be found at https://hellopando.com/acceptable-use-policy/

Agreement: Section A, Section B, Section C.

Authorised Users: Those employees and independent contractors of the Partner who are authorised to access and use the Pando Application, as described here:

> Authorised Users must be employees or independent contractors of the Partner. The User Software will only activate on a user's device if the user has an NHS or valid trust email or other approved account that has passed due diligence checks – e.g. a .gov account. An NHS email account is one of the following: @nhs.net, @(trust). nhs.uk or similar.
>
> In order to ensure secure use of the Pando Application, the Supplier may prohibit access to the Pando Application of any user it suspects is not an employee or independent contractor of the Partner. The Partner shall provide a list of all its employees and independent contractors to the Supplier as requested by the Supplier from time to time for this purpose.
>
> The Partner also agrees to inform the Supplier if an Authorised User cease to be an employee or independent contractor of the Partner so that the Supplier can block his account.
>
> Each Authorised User is required to accept and comply with the Supplier's Acceptable Use Policy. The Acceptable Use Policy will be presented to the Authorised User before they activate the Pando Application and their acceptance of the Acceptable Use Policy is required in order to access the Hosted Software and make use of the Software Services.

Authorised User Personal Data: The Personal Data belonging to Authorised Users as defined in the Data Processing Agreement.

Installed Environment: The hospital, trust, government department, council or practice of the Partner in which the Pando Application will be used and the Software Services provided.

Confidential Information: Information that is proprietary or confidential and is either clearly labelled as such or identified as Confidential Information.

Controller, Processor, Data Subject, Data concerning health, Personal Data, Personal Data breach, Processing and Appropriate Technical and Organisational measures: as defined in the Data Protection Legislation.

Partner Data: The data inputted into the Pando Application by the Partner, by Authorised Users, or by the Supplier on the Partner's behalf.

Data Protection Legislation: The Data Protection Act 2018 implementing the General Data Protection Regulation (EU) 2016/679 as amended or updated from time to time, automatically including any updates made to UK legislation.

Documentation: The documentation published by Supplier that describes the features and functionality of the Software.

Pando Application: The Supplier's proprietary software application in machine-readable object code form only as described in the Documentation including any error corrections, updates, upgrades, modifications and enhancements to it provided to the Partner under this Agreement. The Pando Application consists of the User Software and the Hosted Software.

General Data: The Partner Data that is general in nature, is not Personal Data and not Patient Data or Authorised User Personal Data.

Hosted Software: The element of the Pando Application that runs on remote servers.

Mandatory Policies: Partner's policies relating to patient safety, acceptable use, security and treatment of Patient Data as communicated to the Supplier from time to time.

Patient Data: Data relating to Partner's patients which may contain the patient's Personal Data and data concerning health.

Privacy Policy: The Supplier's privacy policy as updated from time to time which can be found at https://Pandohealth.co/privacy-policy/

Services: The Software Services and /or Professional Services as applicable, given the context in which the term is used.

User Software: The element of the Software that the Authorised User downloads onto their mobile device.

Virus: Anything or device (including any software, code, file or programme) which may: prevent, impair or otherwise adversely affect the operation of any computer software, hardware or network, any telecommunications service, equipment or network or any other service or device; prevent, impair or otherwise adversely affect access to or the operation of any programme or data, including the reliability of any programme or data (whether by rearranging, altering or erasing the programme or data in whole or part or otherwise); or adversely affect the user experience, including worms, trojan horses, viruses and other similar things or devices.

SECTION C – DATA PROCESSING AGREEMENT

1. AUTHORISED USER PERSONAL DATA

For the purposes of this Data Processing Agreement it is acknowledged that the Supplier is the controller of Authorised User Personal Data. The Authorised User Personal Data consist of the data identified in the Privacy Policy. The terms of the Privacy Policy shall apply in relation to the Supplier's processing of the Authorised User Personal Data.

2. PATIENT/PERSONAL DATA

2.1. For the purposes of this Data Processing Agreement it is acknowledged that the Partner is the controller of Personal Data (which may include Patient Data) and the Supplier is the processor of Personal Data. The Personal Data comprises the data set out in the Privacy Policy.

2.2. The terms of the Privacy Policy and the following terms of this Data Processing Agreement will apply to the processing of the Personal Data by the Supplier on behalf of the Partner.

2.3. The Partner and the Authorised Users will provide Supplier with the Personal Data and will ensure that the Personal Data has been collected and transferred to Supplier in full compliance with the Data Protection Legislation.

3. DATA PROCESSING

The Supplier shall:

a) process the Personal Data only to the extent and in such manner as is necessary for the performance of the Services and solely for the purposes set out in the Privacy Policy and shall not process the Personal Data for any other purpose unless the Supplier is required by the laws of any member state of the European Union to process the Personal Data and in such case the Supplier shall promptly notify the Partner of this before performing the processing required by such laws unless such laws prohibit the Supplier from so notifying the Partner;
b) only process the Personal Data in accordance with the Partner's instructions from time to time; and c) only process the Personal Data in the UK and not transfer the Personal Data outside of the UK.

4. SECURITY MEASURES

4.1. The Supplier shall take appropriate technical and organisational measures against the unauthorised or unlawful processing of Personal Data and against the accidental loss or destruction of, or damage to, Personal Data appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures.

4.2. The Supplier will monitor and update, as necessary, the measures it takes in order to ensure the security of Personal Data.

4.3. Personal Data will be encrypted.

5. EMPLOYEES

The Supplier shall ensure:

a) that it takes reasonable steps to ensure the reliability of any of the Supplier's employees who have access to the Personal Data;

b) that access to the Personal Data is limited to only those employees who need access to the Personal Data to meet the Supplier's obligations under this agreement;

c) that access is restricted, in the case of any access by any employee, to such part or parts of the Personal Data as is strictly necessary for performance of that employee's duties;

d) that all of its employees involved with the Services are obliged to keep the Personal Data confidential and have received comprehensive training on the Data Protection Legislation and related good practice.

6. SUB PROCESSORS

6.1. The Supplier may only authorise a third party (sub-processor) to process the Personal Data:

a) subject to the Partner’s prior written consent (which shall not be unreasonably withheld) where the Supplier has supplied the Partner with full details of such sub-processor; and

b) provided that provisions relating to data processing and data protection in the sub-processor's contract are on terms which are substantially the same as those set out in this Data Processing Agreement.

6.2. The Partner hereby authorises the processing of Personal Data by Amazon Web Services who provide hosting services to the Supplier.

6.3. The Supplier shall be liable under and subject to the terms of the Agreement for the performance of any sub-processors appointed pursuant to this clause 6.

7. INDIVIDUALS’ RIGHTS

7.1. If the Supplier receives a request from an individual access to their Personal Data or for the exercise of any of the rights set out in Article 28, para 3(e) of the Council Directive, the Supplier shall: a) notify the Partner within 3 days of receiving such a request; b) provide the Partner with full cooperation and assistance in relation to any such request; and c) not disclose the Personal Data to any individual or to a third party without the Partner’s prior written consent.

7.2. If the Supplier receives any complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either party's compliance with any applicable data protection laws, it shall promptly notify the Partner and it shall provide the

Partner with full cooperation and assistance in relation to any such complaint, notice or communication.

8. COMPLIANCE

8.1. The Supplier shall: a) promptly comply with any request from the Partner requiring the Supplier to amend, transfer or delete the Personal Data; b) assist the Partner, at the Partner's expense, in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications and impact assessments; c) provide, at the Partner's request, a copy of all Personal Data held by it in the format and on the media reasonably specified by the Partner; d) delete or safely return the Partner data on request of the Partner; e) notify the Partner without undue delay if it becomes aware of any unauthorised or unlawful processing, loss of, damage to or destruction of the Personal Data. The Supplier will restore such Personal Data at its own expense; f) maintain complete and accurate records and information to demonstrate its compliance with this Data Processing Agreement; g) maintain the integrity of the Personal Data, without alteration, ensuring that the Personal Data can be separated from any other information created.

9. RECORDS AND AUDIT

9.1. The Supplier will make available to the Partner all information necessary to demonstrate compliance with the obligations laid down under this Data Processing Agreement.

9.2. The Partner is entitled, on giving at least 5 days' notice to the Supplier, to inspect or appoint representatives to inspect all facilities, equipment, documents and electronic data relating to the processing of Personal Data by the Supplier. This requirement to give notice will not apply if the Partner believes that the Supplier is in breach of any of its obligations under this Data Processing Agreement.

Should you need to contact the DPO of Pando Health, you can do so by phone on 020 7052 8285 email dpo@hellopando.com or write to:
300 St John Street, London, EC1V 4PA