The Controller should print a copy of this Data Processing Agreement and the schedules for future reference.

This Agreement is made on May 23, 2018

PARTIES

1. You, the Customer ("**Controller**")

2. **CLANWILLIAM HEALTH (DGL) LIMITED** a company incorporated England and Wales with company number 3020555 whose registered office is at Aurora House, Deltic Avenue, Rooksley, Milton Keynes, Buckinghamshire, MK13 8LW, United Kingdom ("**Processor**"),

(each a "**Party**" and together the "**Parties**").

BACKGROUND

(A) The Controller and the Processor have entered into a services and software licence agreement (the "**Principal Agreement**") pursuant to which the Processor provides certain services to the Controller.

(B) This Agreement takes effect for the Term.

(C) To the extent that the provision of Services involves the processing of Data, the Parties have agreed to enter into this Agreement for the purposes of ensuring compliance with the Data Protection Acts (as defined below).

AGREED TERMS

1. INTERPRETATION

1.1 The following definitions and rules of interpretation apply in this Agreement.

"Business Day"	a day other than a Saturday, Sunday or public holiday in England when banks in London are open for retail business;
"Commencement Date"	the date of this Agreement;
"Data"	means Personal Data and Sensitive Personal Data or Special Categories of Personal Data (as the context requires);
"Data Protection Acts"	means all laws relating to the processing of Data, privacy and security, including without limitation, the Data Protection Act 1998, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which will be superseded by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**General Data Protection Regulation**");
"Normal Business Hours"	9am to 5.30pm GMT on a Business Day;
"Processor System"	any information technology system or systems owned or operated by the Processor to which Data is delivered or on which the Services are performed in accordance with this Agreement;
"Security Breach"	any security breach relating to Data where that breach is likely to result in a high risk to the rights and freedoms of the natural person;
"Services"	the services to be supplied by the Processor to the Controller in connection with the Principal Agreement as set out at Schedule 1;

"Technical and Organisational Security Measures"	shall mean those measures aimed at protecting Data against accidental or unlawful destruction, accidental or unauthorised loss, alteration or unauthorised disclosure of or access to Data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, as set out at Schedule 2; and
"Term"	means the term of the Principal Agreement.

1.2 For the purposes of this Agreement, the terms **"Personal Data"**, **"Data Subject"**, **"controller", "processor"**, **"Processing"** (and **"Process"** and **"Processed"** shall have a corresponding meaning)**,** "**Sensitive Personal Data**" and "**Recipient**" shall have the same meanings as in the Data Protection Acts and the term **Sensitive Personal Data** shall be replaced by the term "**Special Categories of Personal Data**" from 25 May 2018.

1.3 Clause, schedule and paragraph headings are included for convenience only and shall not affect the interpretation of this Agreement.

1.4 The Schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedules.

1.5 Unless the context otherwise requires, words in the singular shall include the plural and vice versa.

1.6 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

1.7 A reference to **writing** or **written** includes faxes and emails sent to those designated persons identified in writing between the Parties.

1.8 References to clauses and schedules are to the clauses and schedules of this Agreement and references to paragraphs are to paragraphs of the relevant schedule.

1.9 In relation to the Processing of the Data, in the case of conflict or ambiguity between:

a) any provision contained in the body of this Agreement and any provision contained in the schedules, the provision in the body of this Agreement shall take precedence; and
b) any of the provisions of this Agreement and the provisions of the Principal Agreement, the provisions of this Agreement shall prevail.

1.10 Any phrase introduced by the terms "other", "including", "include" or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

2. SCOPE

2.1 During the Term, to the extent that the provision of the Services involves the Processing of Data by the Processor, the Parties acknowledge and agree that the Controller shall be responsible as the controller and the Processor shall be responsible as the processor.

2.2 The purposes of the Processing are set out at Schedule 3 and the subject-matter of the Processing is the Data, which includes the specific types of Data and categories of Data Subjects set out at Schedule 3.

3. DATA PROCESSING

3.1 During the Term, the Processor will process the Data in accordance with the terms and conditions set out in this Agreement, and in particular the Processor will:

3.1.1 comply with its obligations as a Processor under the Data Protection Acts;

3.1.2 having regard to the state of the art, costs of implementation (where applicable) and taking into account the nature, scope, context and purposes of the Processing and the risk to the rights and freedoms of Data Subjects posed by the Processing and the information available to the Processor, implement the Technical and Organisational Security Measures, which the Controller and the Processor agree to be appropriate for the purposes of this Agreement;

3.1.3 at the cost of the Controller, insofar as reasonably possible and practicable to do so, assist the Controller in complying with the rights of the Data Subjects as set out in the Data Protection Acts;

3.1.4 without due delay, notify the Controller of any actual Security Breach which does actually affect the Data, after becoming aware of such Security Breach;

3.1.5 agrees that the Data is confidential in nature and the Processor, unless otherwise lawfully directed in writing by Controller, will:

(a) process the Data (on behalf of Controller) exclusively for the provision of the Services and for the purposes which are set out at Schedule 3;

(b) insofar as it is reasonably possible and lawful to do so, process the Data solely in accordance with the instructions of Controller as notified in writing in advance by the Controller, except as required/ permitted to do otherwise by European Union law or the laws of any member state to which the Processor is subject, and (where permitted) the Processor will inform the Controller of such;

(c) take reasonable steps to ensure that each of its employees, officers, representatives, advisers and/or subcontractors engaged in processing the Data ("**Representatives**") will be informed of the confidential nature of the Data and are under an obligation to keep the Data confidential; and

(d) not Process or transfer any Data outside the European Economic Area ("**EEA**") without the prior written consent of the Controller, other than as provided by Clause 4 of this Agreement.

3.2 To the extent that Processor cannot comply with the Controller's instructions pursuant to clause 3.1.5(b) or a change to those instructions (as the case may be) without incurring material additional costs, the Processor shall: (i) immediately inform the Controller, giving full details of the problem; and (ii) cease all processing of the affected Data (other than securely storing that Data) until revised instructions are received.

3.3 The Processor will, at the cost of the Controller and on reasonable notice during Normal Business Hours, give commercially reasonable assistance to the Controller, in ensuring compliance with the Controller's obligations under the Data Protection Acts having regard to the state of the art, costs of implementation (where applicable) and taking into account the nature, scope context and purposes of the Processing and the risk to the rights and freedoms of Data Subjects posed by the Processing and the information available to the Processor.

3.4 The Controller hereby agrees that it will comply with its obligations as a Controller under the Data Protection Acts. In particular, the Controller shall ensure that at all relevant times there is a legal basis for Processing in accordance with the Data Protection Acts to enable the Processor (and such members of the Processor's group of companies) to Process the Data and/or Sensitive Data as pursuant to the Services under this Agreement.

4. SUB-CONTRACTING

4.1 The Controller hereby grants to the Processor authorisation to subcontract its processing functions as it deems necessary in respect of Processing the Data pursuant to this Agreement to any of the third parties listed at Schedule 4, including those third parties based outside the EEA which are also listed at Schedule 4.

4.2 The Processor will inform the Controller of any intended changes concerning the addition or replacement of sub-contractors from such list and the Controller, acting reasonably, will have the right to object to a proposed change within thirty (30) days from receiving written notice from the Processor in accordance with Clause 13 such notice to include evidence as to why the Controller objects. In the event that the Controller objects to any such proposed change, the Processor will have the option to propose an alternative contractor or terminate the Agreement (which will be effective ten (10) days from the Controller exercising its right to object).

4.3 In the event that a sub-contractor is contracted by the Processor to carry out Processing, the Processor will procure (so far as it is within the Processor's control to do so) that such sub-contractor enters into an agreement with the Processor in relation to Processing the Data, the terms of which are similar to, but not less onerous than, the terms of this Agreement.

4.4 The Processor is hereby authorised to transfer the Data to the third parties listed in Schedule 4 as being based outside the EEA on the basis that such transfer is covered by a data transfer agreement in the form of the standard EU Model Clauses Agreement (as set out in the Annex to Commission Decision 2010/87/EU) (the "**Model Contract**") and, in its capacity as data controller, the Controller hereby authorises and requests the Processor to act as its agent for the limited purposes of binding the Controller to the Model Contract with any non-EEA affiliates, vendors and sub-contractors of the Processor to ensure the contractual protection of the Data that is transferred outside the EEA.

5. AUDIT

5.1 Not more than once in any period of twelve months during the Term, the Processor will, at the cost of and on reasonable notice from the Controller during Normal Business Hours:

5.1.1 provide all information necessary; and/or

5.1.2 permit the Controller (or any auditor acting under the authority of the Controller) to carry out an audit or inspection,

to demonstrate the Processor's compliance with its obligations with the Data Protection Acts PROVIDED HOWEVER that any information obtained by the Controller in connection with or in the course of any such audit and any such information provided to or obtained by the Controller shall be maintained by the Controller in the strictest confidence, shall be used solely for the purposes of ensuring that the Processor is complying with its obligations as a Processor under the Data Protection Acts and shall not be used or disclosed for any other purpose.

6. RETURN OR DESTRUCTION OF DATA

6.1 Upon prior written request and at the option and cost of the Controller, the Processor will as soon as reasonably practicable and possible to do so:

a) destroy or return to Controller all Data; and
b) to the extent technically practicable, erase all Data from the Processor System.

6.2 Nothing in Clause 6.1 shall require the Processor to return or destroy Data that the Processor is required to retain by applicable law, or to satisfy the requirements of any laws of the European Union or member state law, regulatory authority or body of competent jurisdiction to which the Processor is subject.

7. LIABILITY

7.1 Neither Party excludes or limits liability to the other Party for:

(a) fraud or fraudulent misrepresentation;
(b) death or personal injury caused by negligence; and/or
(c) any matter for which it would be unlawful for the Parties to exclude liability.

7.2 The Processer's aggregate liability under this Agreement and the Principal Agreement is limited to the amount set out in Clause 9 of the Principal Agreement whether in contract, tort, or for breach of statutory duty or otherwise. For the avoidance of doubt, nothing in this Agreement shall increase such liability to an amount greater than that already agreed pursuant to the Principal Agreement.

7.3 The Controller acknowledges that the Processor is reliant on the Controller for direction as to the extent to which the Processor is entitled to use and process the Personal Data. Consequently, the Processor will not be liable for and the Controller shall indemnify and keep indemnified and defend at its own expense the Processor against all claims, costs (including without limitation court costs and legal fees), damages (direct or indirect), losses or expenses ("**Loss**") suffered or incurred by the Processor or for which the Processor may become liable including and in particular to such arising from:

7.3.1 civil claims where a final award of damages has been granted or which are subject to a court approved settlement; and/or

7.3.2 administrative fines imposed by a supervisory authority and approved by a court of competent jurisdiction,

in each case, except to the extent that any such Loss arises due to the failure by the Processor to comply with any of its obligations under this Agreement or for breach of the Data Protection Acts.

8. TERM AND TERMINATION

8.1 This Agreement shall take effect from the Commencement Date and should continue in full force and effect until the termination or expiry of the Principal Agreement.

8.2 This Agreement may be terminated by either the Controller or Processor with immediate effect by notice in writing to the other Party (the "**Defaulting Party**") if the Defaulting Party is in a material or persistent breach of this Agreement which, in the case of a breach capable of remedy, shall not have been remedied within thirty (30) Business Days from the date of receipt by the Defaulting Party of the written notice specifying this clause, identifying the breach and requiring its remedy.

9. ASSIGNMENT

This Agreement is personal to each Party and neither Party shall assign, transfer, mortgage, charge, subcontract, declare a trust of or deal in any other manner with any of its rights and obligations under this Agreement without the prior written consent of the other Party (which is not to be unreasonably withheld or delayed).

10. FORCE MAJEURE

Neither Party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if that delay or failure results from events, circumstances or causes beyond its reasonable control. In such circumstances, the affected Party shall be entitled to a reasonable extension of the time for performing such obligations. If the period of delay or non-performance continues for 3 months, the Party not affected may terminate this Agreement by giving 21 days' written notice to the affected Party.

11. COUNTERPART

11.1 This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement.

11.2 Transmission of an executed counterpart of this Agreement (but for the avoidance of doubt, not just a signature page) by e-mail (in PDF, JPEG or other agreed format) shall take effect as delivery of an executed counterpart of this Agreement. Each party shall provide the other party with the original of such counterpart as soon as possible thereafter.

12. WAIVER

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, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

13. NOTICE

13.1 Any notice or other communication required or permitted to be given by the Controller under or in connection with this Agreement shall be in writing addressed or sent as follows if to the Processor, if by letter, to Customer Services Manager, Clanwillliam Health DGL Limited Aurora House, Deltic Avenue, Rooksley, Milton Keynes, Buckinghamshire, MK13 8LW, United Kingdom.

13.2 The Processor may provide notices to the Customer electronically, including via email, through any software portal used for the provision of the Software or through a website that the Processor identifies. Notice is given at the date made available by the Processor.

13.3 Any notice or communication shall be deemed to have been received:

a) if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address;
b) if sent by post, at 9.00 am on the second Business Day after posting or at the time recorded by the delivery service; or
c) if sent by email, at 9.00 am on the first Business Day after sending.

13.4 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

14. VARIATION

The Processor may update or amend these terms from time to time by notice to you. Every time the Controller wishes to use the Processor's software or service (as the case may be), it should check these terms to ensure it understands the terms that apply at that time. Unless otherwise agreed in writing with the Processor, the Controller may not vary the terms of this Agreement.

15. RIGHTS AND REMEDIES

Except as expressly provided in this Agreement, the rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

16. SEVERANCE

16.1 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 deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of this Agreement.

16.2 Any provision or part-provision of this agreement is invalid, illegal or unenforceable, the Parties shall negotiate in good faith to amend such provision so that, as amended, it is legal, valid and enforceable, and, to the greatest extent possible, achieves the intended commercial result of the original provision.

17. NO PARTNERSHIP OR AGENCY

Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, nor authorise any Party to make or enter into any commitments for or on behalf of any other Party.

18. ENTIRE AGREEMENT

18.1 This Agreement together with the Principle Agreement constitutes the entire agreement between the Parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

18.2 Each Party acknowledges that in entering into this Agreement it does not rely on, and shall have no remedies in respect of, any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement or the Principal Agreement.

19. GOVERNING LAW

This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of England and Wales.

20. JURISDICTION

Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this agreement or its subject matter or formation (including non-contractual disputes or claims).

IN WITNESS of this Agreement, the Parties have executed this Agreement on the date stated at the beginning of it.

SCHEDULE 1
SERVICES

TECHNICAL SUPPORT OFFERED

- During this Agreement CLANWILLIAM HEALTH will provide the Customer with support between Monday to Friday from 0800 to 2000 UK time (excluding national holidays) & emergency support Saturday 0900 - 1700
- CLANWILLIAM HEALTH shall use its reasonable endeavours to respond to all support-related requests within 4 working hours of a new incident being reported;
- Any non-support related requests will be dealt with entirely at CLANWILLIAM HEALTH's discretion.

RELEASES

- CLANWILLIAM HEALTH shall make available to the Customer any improved version of or updates to the Software that CLANWILLIAM HEALTH shall from time to time make.
- If required by the Customer, CLANWILLIAM HEALTH shall provide training for the Customer in the use of the new release at CLANWILLIAM HEALTH's standard scale of charges for the time being in force as soon as reasonably practicable after the delivery of any new release The new release of the Software shall thereby become the current release of the Software and the provisions of this Agreement shall apply accordingly.
- CLANWILLIAM HEALTH reserves the right to discontinue the Support for prior versions of the Software as notified to the Customer at any time after a superseding version of the Software has been made available to the Customer.

SCHEDULE 2

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Domain	Practices
Organisation of Information Security	**Security Ownership**. Clanwilliam Health have an internal security committee and a Data protection officer **Security Roles and Responsibilities**. Clanwilliam Health staff with access to Customer Data are subject to confidentiality agreements within their contracts. **Risk Management Program**. ISO 27001 framework is used to identify risks to Availability of our services and confidentiality data assets.
Asset Management	**Asset Inventory**. Clanwilliam Health use IS0 27001 frame work for developing an internal asset inventory. **Asset Handling** • Clanwilliam Health regularly review access to assets with departments. • HR issue joiner requests listing requirements for access and also removal off assets for leavers • Monitoring off internal activity is controlled by IBM Qrader • All Assets are have anti virus • Assets with sensitive information are encrypted with Bitlocker or Deslock+
Human Resources Security	**Security Training**. Clanwilliam Health issue all staff with data protection training modules on induction and refresher training every 12 months. Train modules cover Data protection principles, data subject access request, Data Breach and keeping data secure. HR issue starter and leaver forms to IT for removal of access to building, emails, and any IT assets.
Physical and Environmental Security	**Physical Access to Facilities**. Clanwilliam Health requires Fob pass to enter building and fob to enter office. **Physical Access to Components**. Records of employees entering building are logged. Visitors require sign in on book and issues visitor passes. **Protection from Disruptions**. IT Comms room has redundancy with UPS, high availability ISP and firewalls. **Component Disposal**. A data retention policy and procedure has been introduced to comply to GDPR. Shredding is carry out on site and certified
Communications and Operations Management	**Operational Policy**. Clanwilliam Health maintains an Information security management system which contains documents for security access, internet usage , BYOD, email policy, password policy and many others **Data Recovery Procedures** 1. Clanwilliam Health review their backup requirements with departments every 6 months. 2. Off site and on site backups are maintained.

	3. Azure and Keepitsafe are used for Online backups 4. Tests are periodically restored. **Malicious Software**. Clanwilliam Health have Eset Security and anti-virus installed on all IT assets. Qradar SIEM is monitoring the network for malicious activity. **Data Beyond Boundaries** - Clanwilliam Health encrypts data used within data centers and Azure **Event Logging**. Event logs within the network are monitors by Qradar .
Access Control	**Access Policy**. Clanwilliam Health maintains a record of security privileges of individuals having access to Customer Data. These are reviewed with line managers every 6 months. **Access Authorization** 1. Access to data is approved by line manager and HR policies used for joiners and leavers. 2. Clanwilliam Health deactivates authentication credentials from leavers and reviews AD periodically 3. O365 access is managed by IT - Clanwilliam Health ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Customer support personnel are only permitted to have access to Customer Data when needed. - Clanwilliam Health restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Clanwilliam Health instructs Clanwilliam Health personnel to disable administrative sessions when leaving premises Clanwilliam Health controls or when computers are otherwise left unattended. - Clanwilliam Health stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Clanwilliam Health uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Clanwilliam Health requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Clanwilliam Health requires the password to be at least eight characters long with Complexity - Clanwilliam Health ensures that de-activated staff are not granted access
Information Security Incident Management	**Incident Response Process** - Clanwilliam Health have a procedure in place for reporting security breaches. - A major incident policy is in place for the event of such breaches **Service Monitoring**. Clanwilliam Health review monitoring logs periodically.
Business Continuity Management	- Clanwilliam Health maintains a business continuity plan so insure customers have access to services in the event of environmental or physically building access issues.

SCHEDULE 3

1 PURPOSE OF THE PROCESSING

The purposes of the processing are as follows:

1. SOFTWARE UPDATES
2. DRUG INFORMATION UPDATES
3. TECHNICAL SUPPORT SERVICES
4. REMOTE CONNECTION FOR TECHNICAL SUPPORT
5. SUPPORT CALL LOGGING
6. TELEPHONE SUPPORT
7. TRANSFER OF DATA FOR TROUBLESHOOTING

2 DATA

Personal Data

Personal Data may include, among other information, personal contact information such as name, address, telephone or mobile number, fax number, email address, information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title, identification numbers, and social security details.

Special Category Data

Sensitive Personal Data may be processed and may include, racial or ethnic origin, religion, physical or mental health condition and sexual life, notes, prescriptions, maternity, lab results and other medical data.

SCHEDULE 4

LIST OF PROCESSORS ENGAGED BY THE PROCESSOR

Sub-contractor	Function	Location
M247	Data Centre for hosting DGL Platform and data	UK
Esendex	SMS Service Provider	UK
RSA	RSA Keyfobs for secure access to DGL PM hosted platform	UK
New World IT	IT Partner	UK
Codex DSS	CRM System partner	Ireland
Northern Transcript	Transcription Services partner	UK
Ezsmart	Transcription Services partner	India
Egress	Email Encryption	UK
Medisoft (if customer is using Medisoft software)	Integration with Medisoft (ophthalmology software)	UK
Zeiss (If customer is using Medisoft software)	Integration with Zeiss (ophthalmology software)	UK
Spire Sap (only for Spire Customers)	One way integration for appointments and patients with data flowing into DGL PM	UK
HCA Lab, Patient Keeper, CWS & PACs (only on HCA Server)	One-way integration appointments and patients with data flowing into DGL PM	UK
TLC LAB (The London Clinic)	Integration with TLC for diagnostic/lab results	UK
TDL (The Doctors Laboratory)	Integration with TDL for blood results.	UK
World Pay	Integration for card payments	UK

Amplitude	**Integration for clinical outcomes**	**UK**
Pharmacierge	**Integration for medication prescriptions**	**UK**
Healthcode	**Integration for EDI Billing, BUPA lookup and membership lookup.**	**UK**
MMS	**Integration with Clinical Debt Service**	**UK**
Google Calendar	**Integration with Google Calendar on a one-way link (DGL to Google)**	**UK**
Bupa	**Integration with clinician list**	**UK**
Interfax.net	**Ability to send efax**	**UK**
Galway Clinic Link	**Integration into Galway Clinic booking system.**	**Ireland**
Viapost	**Integration for bulk posting service**	**UK**
Cardsave	**Card payments**	**UK**
TLC Diary Link	**Integration with The London Clinic Diary. One-way link (TLC to DGL)**	**UK**
LogMeIn	**Remote support solution**	**UK**
Team Viewer	**Remote support solution**	**Ireland**
Lantel Networks	**Phone system**	**Ireland**

Signed for and on behalf of **CLANWILLIAM HEALTH (DGL) LIMITED**
by its authorised signatory

Eilen Byrne

_____

Authorised Signatory (Signature)

Eileen Byrne

_____

Print name

Signed on behalf of the **CONTROLLER**
by its authorised signatory

Dr Vijay Hajela (May 23, 2018)

_____

Authorised Signatory (Signature)

Dr Vijay Hajela

_____

Print name

Data Processing Agreement - Group 11

Adobe Sign Document History 05/23/2018

Created:	03/29/2018
By:	DGL Support (Clanwilliam Health) (DGL-GDPR@clanwilliamgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAADoSYQh2cdiPZxm2CRbcUxLmVwmSkQAyw

"Data Processing Agreement - Group 11" History

Document created by DGL Support (Clanwilliam Health) (DGL-GDPR@clanwilliamgroup.com)
03/29/2018 - 11:42:29 AM GMT

Document emailed to Dr Vijay Hajela (vijay.hajela@btinternet.com) for signature
03/29/2018 - 11:47:22 AM GMT

Document viewed by Dr Vijay Hajela (vijay.hajela@btinternet.com)
04/01/2018 - 9:50:39 PM GMT- IP address: 82.132.243.124

Document e-signed by Dr Vijay Hajela (vijay.hajela@btinternet.com)
Signature Date: 05/23/2018 - 7:24:19 AM GMT - Time Source: server- IP address: 37.19.29.192

Signed document emailed to DGL Support (Clanwilliam Health) (DGL-GDPR@clanwilliamgroup.com) and Dr Vijay Hajela (vijay.hajela@btinternet.com)
05/23/2018 - 7:24:19 AM GMT