NOTED STANDARD TERMS OF USE

1. INTRODUCTION

1.1 **Service**: Noted Limited (referred to in this agreement as **we**, **us**, **our** and **Noted**) has developed the Noted System. The Noted System is a health software system. The Noted System is made available to users as a service via the internet, called "the **Service**" in this agreement.

1.2 **Application of Terms**: Your agreement with us incorporates these Terms (including the schedules), our Privacy Policy and any Letter of Agreement that you (or the Organisation acting on your behalf) has entered into. The agreement sets out the basis on which we will provide and support, and you (as a user) may access and use, the Service.

1.3 **EU and US users**: By your acceptance of, and agreement to be bound by these Terms, you also agree that you are party to and bound by:

(a) if you are an EU user, schedule 2; and

(b) if you are a US user, schedule 3.

2. SUBSCRIPTION

2.1 **Commencement of Subscription Period**: Your access to and use of the Service is subject to payment of the Fee by you or by someone else on your behalf, such as an organisation of which you are a member that has an agreement for the Service with us covering its members (the **Organisation**). The subscription fee that forms part of the Fee is payable monthly in advance and is calculated based on the number of Users. Unless we deduct the Fee from your account or it is paid by the Organisation, you must pay the Fee by the 20th of the month following the date of invoice and electronically in cleared funds without any set-off or deduction.

3. PROVISION OF SERVICE

3.1 **Service**: Subject to this agreement, we will provide the Service to you during the Subscription Period. You acknowledge that:

(a) we do not provide you with internet access or any computer equipment or software required to access the Service; and

(b) we may change the Service from time to time to provide bug fixes and/or new, replacement or improved features or functionality.

3.2 **Optional Services**: We may also from time to time offer optional services relating to the Service, such as special purpose software applications or reports. You may request any such services by contacting us. We will be under no obligation to provide such services until we have provided notice confirming our acceptance of your request.

3.3 **Grant of Rights**: Subject to this agreement, we grant you a non-exclusive, non-transferable, non-sub-licensable right to use the Service during the Subscription Period solely in connection with your lawful internal business purposes (**Permitted Purpose**).

3.4 **Additional Fees**: You acknowledge that we may charge additional fees if:

(a) as part of the ordinary development of its product, we add further functionality to the Noted System or

(b) at your or the Organisation's request, we develop additional functionality that is outside our planned product development and is not applicable to our other clients.

3.5 **Reasonable Price**: Where we intend to charge an additional fee under clause 3.4(b), the parties, or we and the Organisation as the case may be, will enter into good faith negotiations to determine a reasonable price for the additional functionality.

3.6 **Collaboration**: You agree to work collaboratively with us to, among other things, provide us with data and feedback about the Service and the Noted System in a timely manner.

4. YOUR RESPONSIBILITIES

You must:

4.1 **No Other Use**: not use the Service for any purpose other than the Permitted Purpose;

4.2 **No resale**: not resell or make available the Service to any third party, or otherwise commercially exploit the Service, without our prior written consent;

4.3 **Third party information**: ensure you have included such statements in your privacy policy as may be required in connection with any use of the Service, and ensure you have obtained any necessary consents and authorisations from individuals for the collection, storage, disclosure and use of all data and other information obtained from and/or relating to them which you store using the Service;

4.4 **Login and Password**: keep your log-in name and password secure and secret, and notify us immediately if you become aware of any unauthorised person accessing the Service using your log-in name and password;

4.5 **Access**: not permit anyone other than you to access or use the Service without our prior written consent;

4.6 **Instructions**: comply with our reasonable instructions relating to access to, and use of, the Service;

4.7 **Laws**: comply with all applicable laws when accessing and using the Service, including but not limited to all applicable laws relating to confidentiality and privacy;

4.8 **Dealings**: not sub-license, assign, transfer, lease, rent, distribute or resell the Service, or any rights to access or use the Service, to any other person without our prior written consent;

4.9 **Security and Integrity**: not attempt to undermine the security or integrity of our computing systems or networks (including the Noted System) or, where the Service is hosted by a third party, that third party's computing systems and networks;

4.10 **Impairment:** not use, or misuse, the Service in any way which may impair the functionality of the Service, or other systems used to deliver the Service or impair the ability of any other user to use the Service;

4.11 **Unauthorised Access**: not attempt to gain unauthorised access to any materials other than those to which you have been given express permission to access;

4.12 **Harmful/Offensive/Illegal Content**: not transmit, or input into the Service, any:

(a) files that may damage any other person's computing devices or software;

(b) content that may be offensive; or

(c) material or Data in violation of any law (including Data or other material protected by copyright or trade secrets which you or the relevant User do not have the right to use);

4.13 **Copy or Modify etc**: not, except as and to the extent permitted by law, copy, reproduce, translate, adapt, modify or create derivative works of the Service or any computer programs used to deliver the Service by any means or in any form without our prior written consent; and

4.14 **Reverse Engineering**: not reverse assemble or decompile the whole or any part of the Service or any computer programs used to deliver the Service.

5. OUR RESPONSIBILITIES

5.1 **Care, Skill and Diligence**: We will, in providing the Service and any other services under this agreement, act with reasonable care, skill and diligence.

5.2 **Service Availability**: We will use reasonable endeavours to ensure that the Service is available and providing (in all material respects) the functionality described in the Specifications at all times other than when we need to suspend access to the Service in order to carry out any software upgrades or other maintenance. If for any reason we have to interrupt the Service for longer periods than we would normally expect, we will use reasonable endeavours to publish in advance details of such activity. We do not guarantee that your access to, or use of, the Service will be uninterrupted, error or virus free.

5.3 **Support**: In the case of technical problems you must make all reasonable efforts to investigate and diagnose problems before contacting us. If you still need technical help, email us at support@noted.com, or contact us via our Help and Support page.

6. PRIVACY

6.1 Access to and use of all Personal Information in connection with this agreement is governed by this agreement, which shall include:

(a) if you are an EU user of the Service, schedule 2 to these Terms; or

(b) if you are a US user of the Service, schedule 3 to these Terms.

If schedule 2 or 3 applies to you, and there is any inconsistency between the terms in these Terms or Privacy Policy and the relevant schedule, the terms of the schedule shall apply.

6.2 We collect and process your Personal Information and the Personal Information of your Users when you (or your Users, as applicable) access or use the Service. In order to provide you with the Service (and improve on it), we may also collect certain information about the performance of the Service and the Noted System and your (and your Users') use of the Service and Noted System.

6.3 We may access, process and/or disclose Personal Information in order to: (i) provide you with the Service; (ii) analyse and monitor use of the Service; (iii) comply with the law or legal proceedings served on us (including any notification and reporting obligations and any access directions, imposed on us by Government agency); (iv) enforce and investigate potential breaches by you of the agreement or any other unauthorised use of the Service; (v) protect our rights, property, or the safety of our employees, customers or the public; and (vi) for any other purpose we specifically tell you about or that you have otherwise authorised. By agreeing to this agreement, you also consent to the way we access process and/or disclose your (and, if applicable, your Users') personal information.

6.4 We may also access and process Personal Information of users in order to inform users of any products, software, services or information that we believe such users may be interested in.

6.5 We work with third party service providers who provide various services for us in connection with the Service (including, hosting and maintenance services). These third parties may have access to, or process, Personal Information as part of providing those services for us. We limit the Personal Information provided to these service providers to that which is reasonably necessary for them to perform their functions,

and our contracts with them require them to maintain the confidentiality of such information.

6.6 We utilise the services of overseas entities in Australia and Germany to provide us with hosting and maintenance services. Consequently, we may transfer Personal Information to parties located in these other countries. Although we will endeavour to ensure that your Personal Information is treated securely and in accordance with this agreement as well as applicable data protection laws, you acknowledge that some of these countries may not have an equivalent level of data protection laws as those in New Zealand.

6.7 You have the right to ask for a copy of any Personal Information we hold about you, and to ask for it to be corrected if you think it is wrong. If you would like to ask for a copy of your personal information, or have it corrected or deleted from our records, please contact us at https://www.noted.com/privacy-statement.

6.8 You must comply with all applicable data privacy laws in connection with your collection and use of any Personal Information of any person. You will not (and, if applicable, will ensure your Users do not) use the Services: (i) to collect Personal Information about third parties other than as expressly provided for in this Agreement, including without limitation, e-mail addresses; or (ii) in a way that violates (or may be considered inconsistent with) the privacy, rights or civil liberties of any person (including in a way that prevents the exercise of them).

6.9 You warrant that you have obtained any necessary consents and authorisations from individuals (including your Users) for the collection, storage, disclosure and use of all data and other information (including personal information) obtained from and/or relating to them which you store using the Service

7. Data Security

7.1 **Our acknowledgements**: It is acknowledged and agreed by us that:

(a) all of your Data, including any Data: (i) uploaded, submitted, posted, transferred, transmitted, or otherwise provided or made available by or on behalf of you or any of your Users for processing by or through the Service; or (ii) collected, downloaded, or otherwise received you or the Service for you or any of your Users, will be owned exclusively by you (or your Users, as applicable) and all rights not expressly granted to us in this agreement are reserved to you or your users (as applicable).

(b) We will not use Data for any purpose other than as specified in this agreement, and otherwise as required to comply with our obligations under this agreement and applicable laws.

(c) Data will not be disclosed, sold, assigned, leased or otherwise disposed of to third parties, except as expressly provided for in this agreement.

(d) If you request, upon reasonable notice to us, we will provide you with the latest list of Supplier's personnel that have access to Data.

7.2 **Your acknowledgements**: You acknowledge and agree that:

(a) Subject to your rights under applicable laws, your right to edit the Data is contingent on full payment of any Fees payable when due. Your right to read-only access to the Data will be unaffected, subject to deletion of the Data under this agreement.

(b) While we adhere to best practice policies and procedures to keep your Data secure and confidential and have entered into appropriate arrangements requiring our service providers to keep your Data secure and confidential, we note that the internet is inherently insecure, and cannot guarantee that there

will never be any unauthorised access to, or loss of, your Data. We expressly exclude liability for any loss of Data no matter how caused;

(c) You consent to the collection, transfer, manipulation, storage, disclosure and other uses of your Data for the purposes of delivering the Service and as otherwise expressly provided for in this agreement.

(d) Data input into the Service during the Trial Subscription will be deleted if you fail to upgrade to a Paid Subscription within 120 days of the Commencement Date.

(e) We are not liable, in any circumstances, for breaches of the applicable laws caused by you.

7.3 **Data security**: We are committed to protecting the security of your Data. We have implemented and will maintain and follow appropriate technical and organizational measures intended to protect Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. Our data security measures are summarised in schedule 1.

7.4 **Anonymous Data**: Solely as necessary to provide the Service to you, including as necessary to ensure that the Service incorporates all features and capabilities required to provide the Service in accordance with this agreement, you grant to us a non-exclusive royalty-free worldwide and irrevocable license permitting us to copy, anonymize, aggregate, process and display Data to derive anonymous statistical and usage data, and data about the functionality of the Service and the Noted System, provided such data cannot be used to identify you or any of your Users (**Anonymous Data**).

7.5 **Aggregated Data**: Solely as necessary to provide the Service to you, including as necessary to ensure that the Service incorporates all features and capabilities required to provide the Service in accordance with this agreement, we may adapt or modify Anonymous Data or combine Anonymous Data with or into other similar data and information available, derived or obtained from other subscribers, licensees, users, or otherwise (when so adapted, modified, combined or incorporated, referred to as **Aggregate Data**).

7.6 **Further rights**: We may also use Anonymous Data and Aggregate Data to enable us to inform you of any products, software, services or information that we believe you may be interested in.

7.7 **International transfer of Data**: We may store Data in servers of our service providers, which may be located in a different country to us, and may access that Data in either New Zealand, Australia, Germany or the location of any of our Affiliated Companies from time to time.

7.8 **Indemnity**: You indemnity us against any liability, claims and costs (including the actual legal fees charged by our solicitors) arising from any claim by a third party that our possession or use of any Data in accordance with its rights under this agreement:

(a) infringes a third party's Intellectual Property Rights or privacy rights;

(b) is defamatory, objectionable, obscene or harassing;

(c) is unlawful in any way; or

(d) will otherwise result in us being in breach of this agreement.

8. INTELLECTUAL PROPERTY AND CONFIDENTIALITY

8.1 **Ownership**:

(a) We (or our licensors) own all Intellectual Property Rights in or relating to the Service and the Noted System. We will also own any new Intellectual

Property Rights in anything developed by or on behalf of us in the course of providing, supporting or maintaining the Service as such rights arise.

(b) As between you and us, you own the Data.

8.2 **Contributions or Suggestions**: In the course of your use, you may make contributions or suggestions relating to the Service. To the extent that any such suggestions or contributions result in the creation of new Intellectual Property Rights relating to the Service, such Intellectual Property Rights will be owned by us. If requested, you agree to sign such documents as might be requested to assign such Intellectual Property Rights to us.

8.3 **Confidentiality**: Each party must, unless it has the prior written consent of the other party:

(a) keep confidential at all times the Confidential Information of the other party;

(b) effect and maintain adequate security measures to safeguard the other party's Confidential Information from unauthorised access or use; and

(c) disclose the other party's Confidential Information to its personnel or professional advisors on a need to know basis only and, in that case, ensure that any personnel or professional advisor to whom it discloses the other party's Confidential Information is aware of, and complies with, clauses 8.3(a) and 8.3(b).

8.4 **Exclusions**: The obligation of confidentiality in clause 8.3(a) does not apply to any disclosure or use of Confidential Information:

(a) for the purpose of performing a party's obligations, or exercising a party's rights, under the agreement;

(b) as required by law (including under the rules of any stock exchange);

(c) which is publicly available through no fault of the recipient of the Confidential Information or its personnel;

(d) which was rightfully received by a party from a third party without restriction and without breach of any obligation of confidentiality; or

(e) by us if required as part of a bona fide sale of our business (assets or shares, whether in whole or in part) to a third party, provided that we enter into a confidentiality agreement with the third party on terms no less restrictive than this clause 8.

9. LIABILITY

9.1 **No Warranties**: The provision of, access to, and use of, the Services is on an "as is" basis and at your own risk. To the extent permitted by law, we disclaim and exclude all representations, warranties and conditions, whether express, implied or statutory, relating to the Service and any other services we supply to you under this agreement. Without limiting the foregoing:

(a) we do not warrant that the access to or use of the Service will be uninterrupted or error free;

(b) we do not warrant that the Services will meet your requirements or that it they will be suitable for any particular purpose; and

(c) all warranties of fitness for purpose and non-infringement are excluded.

9.2 **Consumer Guarantees**: You agree and represent that you are acquiring the Service, and accepting the agreement, for the purpose of trade and that the Consumer Guarantees Act 1993 and any other applicable consumer protection legislation does not apply to the supply of the Service or these Terms. You and we agree it is fair and reasonable that this clause 9.2 applies.

9.3 **Adequacy**: You must satisfy yourself as to the adequacy, appropriateness and compatibility of the Service for your requirements.

9.4 **No Liability**: To the maximum extent permitted by law and unless expressly provided otherwise in schedule 2 or 3, we will have no liability to you (or any other person) under or in connection with this agreement (whether in contract, tort or otherwise), for any Losses resulting, directly or indirectly, from any use of, or reliance on, the Service.

9.5 **Back-stop Liability Provisions**: If, notwithstanding clauses 9.1 to 9.4, we are liable to you under or in connection with this agreement, the Service or the Data then, to the fullest extent permitted by applicable law:

(a) we will have no liability to you in respect of any:

(i) indirect, consequential or special Losses suffered or incurred by you;

(ii) loss of data, profits, revenue, business or goodwill; or

(iii) Losses suffered or incurred by you, to the extent to which these result from any act or omission by you or your Users (including any breach of this agreement); and

(b) our maximum aggregate liability under or in connection with this agreement, the Data or relating to the Service, whether in contract, tort (including negligence), breach of statutory duty or otherwise, must not exceed an amount equal to 12 months' subscription Fees.

9.6 **Indemnity**: You agree to indemnify us from and against any claim, cost or liability, including reasonable legal fees, arising directly or indirectly out of the use of the Service by you or any person for whom you are responsible in law.

10. CANCELLATION, SUSPENSION AND TERMINATION

10.1 **Cancellation by you**: You may cancel your Subscription at any time by giving us notice in accordance with the process outlined via the Service. If you cancel your Subscription before the end of a month for which you have already paid, the Service will end immediately and you will not be charged again.

10.2 **Suspension or Termination of Access to Service**: Subject to your rights to access Data under applicable laws and these terms of use (including the applicable schedules), we may terminate your use of the Service at our sole discretion, for any reason, at any time, including (but not limited to):

(a) your Trial Period has expired, you have not upgraded to a Paid Subscription, and it is within 120 days of the Commencement Date;

(b) you have cancelled your Subscription;

(c) any Fees or charges payable by or on your behalf under this agreement are 10 Business Days or more overdue for payment; or

(d) you have committed a material breach of this agreement,

and you have failed to pay those Fees or charges in full or remedy that material breach to our satisfaction within 10 Business Days of receiving a notice from us specifying the relevant non-payment or breach and advising our intention to suspend or terminate access to the Service.

10.3 **Reactivation**: Where 10.2 applies, we will suspend the Service for up to 90 days. You may reactive your Subscription, subject to our agreement to do so, during this time. During the suspension of the Service, you will not have editable access to your Data, but you will be able to export your Data in a common electronic form, such as JSON. We do not warrant that the format of the Data will be compatible with any software. At

the end of 90 days, unless you have reactivated your Subscription, your Data will be deleted and will not be able to be recovered.

10.4 **Effect of termination or expiry**:

(a) Termination or expiry of this agreement does not affect either party's rights or obligations that accrued before that termination.

(b) On termination or expiry of this agreement, unless your Fees have been paid by the Organisation, you must pay all Fees for the provision of the Service prior to that termination.

10.5 **No refund**: We are not responsible for any loss you suffer, and no compensation is payable by us to you, as a result of the suspension and/or termination of this agreement for whatever reason, and you will not be entitled to a refund of any Fees that you or the Organisation have already paid.

10.6 **Survival**: Clauses which, by their nature, are intended to survive termination of this agreement continue in force, including clauses 6 (Privacy), 8 (Intellectual Property and Confidentiality) and clause 9 (Liability). This includes clauses in the schedules, as applicable.

11. AMENDMENTS

11.1 **Amendments Proposed via Service:** We may from time to time request that you accept certain amendments to this agreement (save for the provisions of Schedule 2 which may not be modified as set out in that Schedule) when you log-in to use the Service. Any such amendments will be effective if you accept them in the manner provided for acceptance. If you do not accept any such amendments, you will not be able to use the Service for the time being and you must contact us, in which case we will discuss the amendments with you and, if you will not agree to the amendments, either withdraw the amendments, agree revised amendments with you, or allow you to terminate this agreement.

12. GENERAL

12.1 **Governing Law and Jurisdiction:** These Terms, save for the terms in schedules 2 and 3, are governed by the laws of New Zealand. You and we submit to the non-exclusive jurisdiction of the New Zealand courts in respect of all matters relating to them. The terms in schedules 2 and 3 (and their annexes) shall be governed by the laws set out in the relevant schedule.

12.2 **Force Majeure**: Neither party is liable to the other for any failure to perform its obligations under the agreement to the extent caused by Force Majeure.

12.3 **Dispute Resolution:** The parties agree to attempt to amicably resolve any dispute concerning any rights or obligations of either of them under this agreement by doing the following:

(a) the party claiming a dispute has arisen will give written notice to the other specifying the nature and particulars of the dispute and will give a reasonable period of time for the other party to remedy the dispute; and

(b) the parties will endeavour, in good faith, to amicably negotiate and resolve the dispute between themselves.

12.4 **Termination**: If the parties fail to amicably resolve any such dispute within a reasonable period after the issuance of written notice, the party who issued the notice is entitled to terminate the agreement by giving written notice to the other party.

12.5 **Entire Agreement**: These Terms (including any schedules to it) together with the Privacy Policy and any Letter of Agreement, record the entire understanding and agreement of the parties relating to the matters dealt with in this agreement. This

agreement supersedes all previous understandings or agreements (whether written, oral or both) between the parties relating to these matters.

12.6 **Assignment**: Neither party may transfer, sell, or assign this agreement, or any of its rights, obligations or duties under, without the prior written consent of the other party, such consent not to be unreasonably withheld.

12.7 **Relationship**: The relationship between the parties under this agreement is that of customer and service provider and nothing expressed or implied in this agreement constitutes either party or their personnel as the partner, employee or officer of, or as a joint venturer with, the other party

12.8 **Waiver**: No waiver of any breach, or failure to enforce any provision, of this agreement at any time by either party will in any way affect, limit or waive that party's right to subsequently require strict compliance with this agreement.

12.9 **Costs:** Each party shall cover its own costs incurred by it in connection with the negotiation, and execution of this agreement.

12.10 **Further Assurances**: Each party will do all things and execute all documents reasonably required to give effect to the provisions and intent of this agreement.

13. DEFINITIONS AND INTERPRETATION

13.1 **Definitions:** In this agreement, unless the context indicates otherwise:

agreement means these Terms, schedule one and any other schedules relevant to you, our privacy Policy, and any Letter of Agreement executed by you (or by the Organisation that pays the Fees on your behalf);

Business Day means Monday to Friday (New Zealand time) other than any public holiday observed in Wellington, New Zealand;

Data means any data input by you into the Service and any information or data the Service generates for you based solely on the input of such data;

Commencement Date means the date that you commence using the Service;

EU user means users subject to EU law or otherwise based in the EU.

Fees means the fees set out on our website or in the applicable Letter of Agreement;

Force Majeure means an event that is beyond the reasonable control of a party, excluding an event to the extent that it could have been avoided by a party taking reasonable steps or reasonable care or a lack of funds for any reason.

including and similar words do not imply any limitation;

Intellectual Property Rights means trade marks, rights in domain names, copyright, patents, registered designs, circuit layouts, rights in computer software, databases and lists, rights in inventions, confidential information, know-how and trade secrets, and operating manuals and training manuals;

Losses includes any loss, damage, liability, damages, cost or expense, including legal costs on a solicitor and own client basis;

Noted System means our electronic medical record system called Noted;

Organisation has the meaning set out in clause 2.1.

Paid Subscription means a subscription to the Service for a monthly fee;

Period means the duration of this agreement as selected by you on registering for the Service or set out in the applicable Letter of Agreement;

Permitted Purpose is defined in clause 3.3;

Personal Information has the meaning to that term in the Privacy Act 2020;

Privacy Policy means our privacy policy which can be accessed at https://www.noted.com/privacy-statement, as updated by us from time to time;

Service means the service involving the provision of access to the Noted System via the internet and all related activities performed by us as described on our website or in the applicable Letter of Agreement;

Specifications means the specifications published by us or made available on our website (or any replacement URL) or set out in the Letter of Agreement describing the features and functionality of the Service, as updated from time to time;

Letter of Agreement means any quote, Letter of Agreement, or services agreement to which these Terms are attached or incorporated by reference;

Subscription Period means the period commencing on the Commencement Date until termination, provided all fees payable in respect of your use of the Service are made;

Terms means these Standard Terms of Use and includes any schedules to them;

Trial Period means a 30 day period from the Commencement Date;

Trial Subscription means a free subscription to the Service for the Trial Period;

User means, if you are an Organisation, each person registered by you to use the Service;

US user means users subject to US law; and

you means you or the person on whose behalf you are entering into the agreement.

13.2 **Terms**: Save for the terms in schedules 2 and 3, if these Terms are inconsistent in any respect with the applicable Letter of Agreement, the Letter of Agreement prevails. The terms of schedules 2 and 3 (as applicable) shall prevail over any inconsistent terms.

SCHEDULE 1 – DATA SECURITY

Organization of Data security	**Security appointments** Noted has appointed one or more security officers responsible for coordinating and monitoring its security rules and procedures. **Roles and responsibilities** Noted personnel with access to Data are subject to confidentiality obligations.
Asset management	**Inventory**. Noted maintains an inventory of all media on which Data is stored. Access to the inventories of such media is restricted to Noted personnel authorized in writing to have such access. **Handling** ▪ Noted imposes restrictions on printing Data and has procedures for disposing of printed materials that contain Data. ▪ Noted personnel are prohibited from storing Data on portable devices, remotely accessing Data, or processing Data outside Noted's facilities unless authorization is received from you to do so.
Personnel	**Checks** Noted undertakes criminal and employment background checks on each of its employees. **Training**. Noted informs its personnel about relevant security procedures and

	their respective roles. Noted also informs its personnel of possible consequences of breaching the security rules and procedures. Noted will only use anonymous data in training.
Physical and environmental security	**Encryption** Noted diligently selects modern encryption methods when designing its applications. **Facilities** Dedicated hosting environment, no systems are shared with other parties ▪ Replicated filesystem from live to backup systems. ▪ Real-time database replication from live to standby systems. ▪ Database and filesystem snapshots are taken every 10 minutes for point in time restoration; these are aged out over several weeks. Weekly snapshots kept permanently. ▪ Encrypted and secure offsite backups. **Protection from disruptions** ▪ Noted uses a variety of industry standard systems to protect against loss of Data due to power supply failure or line interference. ▪ Noted uses protocols and technologies that protect against DDoS attacks. The Services are available to the internet via AWS ALB.
Communications and operations management	**Operational Policy** Noted maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Data. **Data Recovery Procedures** ▪ Noted undertakes daily data backups. ▪ Data is restored during each fortnightly release. ▪ Noted has specific procedures in place governing access to copies of Data. ▪ Noted reviews Data recovery procedures at least every six months. ▪ Noted logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which Data (if any) had to be input manually in the data recovery process. **Event Logging** Noted logs access and use of information systems containing Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Deletion of Data	● Noted ensures that all Data is deleted from the Service and its systems once it is no longer necessary to retain it. ● On termination of this agreement, Noted will delete all Data that has not already been deleted within 60 days of the date of termination or expiry.
Access Control	**Policy** Noted maintains a record of security privileges of individuals having access to Data.

	Authorization ▪ Noted maintains and updates a record of personnel authorized to access Noted systems that contain Data. ▪ Noted deactivates authentication credentials that have not been used for a period of time not to exceed six months. ▪ Noted identifies those personnel who may grant, alter or cancel authorized access to data and resources. ▪ Noted ensures that where more than one individual has access to systems containing Data, the individuals have separate identifiers/log-ins. ▪ Technical support personnel are only permitted to have access to Data when needed. ▪ Noted restricts access to Data to only those individuals who require such access to perform their job function. **Confidentiality** ▪ Noted instructs Noted personnel to disable administrative sessions when leaving premises Noted controls or when computers are otherwise left unattended. ▪ Noted stores passwords in a way that makes them unintelligible while they are in force. **Authentication** ▪ Noted uses industry standard practices to identify and authenticate users who attempt to access information systems. ▪ Where authentication mechanisms are based on passwords, Noted requires that the passwords are renewed regularly. ▪ Where authentication mechanisms are based on passwords, Noted requires the password to be at least eight characters long. ▪ Noted monitors repeated attempts to gain access to the information system using an invalid password. ▪ Noted uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network design** Noted has controls to avoid individuals assuming access rights they have not been assigned to gain access to Data they are not authorized to access.
Incident Management	**Incident response process** ▪ Noted maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. ▪ For each security breach that is a “Security Incident” notification issued by Noted, as described in the “Security Incident Notification” section below.
Penetration testing	Noted tests all code for security vulnerabilities before release, and regularly scans our network and systems for vulnerabilities.
Business continuity management	▪ Noted maintains emergency and contingency plans for the facilities in which Noted information systems that process Data are located. ▪ Noted ’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Data in its original or

	last-replicated state from before the time it was lost or destroyed.
Business continuity testing	**Your testing** We will, at your cost, participate in your Business Continuity Management plan testing annually upon your request. **Our testing** We will test our Business Continuity Management plan(s) in accordance with our current practices at the date of this agreement and will promptly provide to you a copy of a summary of the test results, as such test results apply to you and the Service. We will reasonably cooperate to address any of your input regarding the test. **Audit right** You may (at your own cost and on reasonable notice to us) audit our Business Continuity Management plan(s) testing annually.
Security incident notification	Noted will monitor the Service and systems under its control for any actual or potential security incidents/vulnerabilities or performance issues. If Noted becomes aware of any unlawful access to any Data stored on the Noted System, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Data (each a "Security Incident"), Noted will : ● within 72 hours or less, notify you (in writing) of the Security Incident; ● promptly investigate the Security Incident and provide you with detailed information about the Security Incident; and ● promptly take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Notification(s) of Security Incidents will be delivered to one or more of your administrators by any means Noted selects, including via email. It is your sole responsibility to ensure your administrators maintain accurate contact information on their Noted account profile. Noted's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Noted of any fault or liability with respect to the Security Incident. You must notify Noted promptly about any possible misuse of its accounts or authentication credentials or any security incident related to Noted.

SCHEDULE 2- DATA PROCESSING AGREEMENT

BACKGROUND

A. You (the **Controlle**r) and Noted Limited (the **Processor**) have entered into the Processor's Terms of Service for the provision of online services by the Processor for the Controller.

B. As required by Applicable Privacy Laws, the Controller and the Processor have agreed to enter into this Agreement for the protection of the personal data that may be processed by the Processor in providing the Services.

C. By this Agreement, the Controller authorizes the Processor to process the Controller Personal Data transferred to it in accordance with the Terms of Service and this Agreement.

AGREEMENT

1 DEFINITIONS

1.1 **Definitions**: Unless the context otherwise requires:

Agreement means this data processing agreement.

Applicable Privacy Laws means the laws protecting the right to privacy with respect to the processing of personal data applicable to the Controller and the Processor, including the General Data Protection Regulation (EU) 2016/679 (**GDPR**).

Business Day means a day other than a Saturday or Sunday or public holiday on which banks are open for commercial business in the country of the Processor.

Controller Personal Data means any Personal Data in respect of which the Controller is a data controller, including the type of Personal Data and categories of Data Subjects referred to in the Terms of Service, and which is processed by the Processor on the instructions of the Controller.

Cross-Border Data Transfer means any transfer of Controller Personal Data to recipients located in a Third Country.

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Controller Personal Data.

Regulatory Bodies means those government departments and regulatory, statutory and other bodies, entities and committees (including any supervisory authority) which, whether under statute, rule, regulation, code of practice or otherwise, are entitled to regulate, investigate or influence the matters relating to the security of data, Personal Data, privacy protection or other laws.

Services means the services as described in the Terms of Service.

Standard Contractual Clauses or **SCC** means the standard contractual clauses set out in schedule 1 to this Agreement, for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these.

Subprocessor means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract.

technical and organisational security measures means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Terms of Service means the Business Associate's terms of service and its schedules, its Privacy Policy and any Letter of Agreement.

Transfer shall mean making Controller Personal Data accessible to any person other than the Data Subject, including, but not limited to the active transfer of the data, permitting access, also remotely, sharing and publishing.

Third Country means a country or territory which is not a Member State of the European Union or EEA.

1.2 **Personal Data**, **special categories of data**, **process/processing**, **controller**, **processor**, **Data Subject** and **supervisory authority** shall have the same meaning as in 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.

1.3 **data exporter** means the controller who transfers the personal data; **The data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of this Agreement and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC.

1.4 All other capitalised terms used in this Agreement shall have the meanings given to them in the Terms of Service.

1.5 **Interpretation**: In this Agreement where the context permits:

1.5.1 reference to a party shall include that party's executors, administrators, successors and assigns;

1.5.2 reference to a statute or regulation shall include all amendments and re-enactments thereof;

1.5.3 writing includes electronic communications (including email) and written has a corresponding meaning; and

1.5.4 the clause headings are inserted for ease of reference only and do not affect the construction of this Agreement.

2 Data Controller and Data Processor

2.1 **Data Controller**: The Processor acknowledges that, in respect of the Controller Personal Data and for the purposes of the Applicable Privacy Laws, the Controller (and each group company of the Controller) is the data controller. The Controller agrees to comply with its obligations under this Agreement and (as data controller) under all Applicable Privacy Laws.

2.2 **Privacy notices**: The Controller is solely responsible for all data controller obligations under Applicable Privacy Laws, including providing any required notices and obtaining any required consents, and for the processing instructions that it gives to the Processor.

2.3 **Controller warranties**: The Controller warrants that:

2.3.1 no contractual obligations prohibit the processing of the Controller Personal Data as described in the Terms of Service and this Agreement; and

2.3.2 the production, collection, and processing of Controller Personal Data has been and will continue to be carried out in accordance with the Applicable Privacy Laws.

2.4 **Appointment as Data Processor**: The Controller appoints the Processor as a data processor of the Controller Personal Data, and the Provider accepts the appointment and agrees to comply with its obligations under this Agreement.

3 Data processing

3.1 **Principles**: Controller Personal Data shall be processed under the general principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

3.2 **Processing restrictions**: Subject to clause 3.3, the Processor shall ensure that all Controller Personal Data is processed only:

3.2.1 according to the instructions of the Controller, which shall include for the purposes of providing the Services as described in the Terms of Service;

3.2.2 in accordance with this Agreement;

3.2.3 in compliance with Applicable Privacy Laws; and

3.2.4 except as otherwise specified in clause 7, within the European Union or a Third Country which ensures an adequate level of protection as indicated by the decision of the European Commission taken pursuant to article 25(6) of the Directive or article 45, § 3, of the GDPR.

3.3 **SCC**: If the Processor is located in a Third Country, and is not an “adequate” country (pursuant to the GDPR), sign the Standard Contractual Clauses as set out in schedule 1 to this Agreement. It is acknowledged that the Standard Contractual Clauses shall only apply to the Processor if the Processor is based outside of a country that has gained adequacy status under the GDPR. For clarity, New Zealand holds adequacy status under the GDPR.

3.4 **Outside of instructions**: The Processor may process Controller Personal Data outside of the Controller’s instructions if laws to which the Processor is subject require it. The Processor shall notify the Controller if it is of the opinion that any instruction provided by the Controller is in breach of any Applicable Privacy Law.

3.5 **Processor personnel**: The Processor will ensure that its personnel:

3.5.1 have undertaken training on Applicable Privacy Laws relating to handling Personal Data and how it applies to their particular duties; and

3.5.2 are aware both of the Processor’s duties and their personal duties and obligations under Applicable Privacy Laws and this Agreement.

4 Cooperation obligations

4.1 **Assistance**: The Processor shall take any steps reasonably requested by the Controller to assist the Controller to demonstrate compliance with its obligations under Applicable Privacy Laws, including to assist and support the Controller:

4.1.1 in the event of an investigation or other control measures or by any Regulatory Body to the extent that such investigation relates to Controller Personal Data;

4.1.2 in the event of the exercise of any claims by Data Subjects or third parties related to the processing under this Agreement;

4.1.3 in complying with the rights of Data Subjects, including the right to obtain transparent information, the right to access, rectify, and erase their personal data, restrict, or object to, the processing of their personal data, exercise their right to data portability;

4.1.4 in notifying, consulting with and obtaining approvals from Regulatory Bodies where required; and

4.1.5 in performing data protection impact assessments.

4.2 **Data Subject rights**:

4.2.1 The Processor shall promptly comply with any request from the Controller requiring the Processor to access, amend, transfer or delete any Controller Personal Data.

4.2.2 The Processor must inform the Controller promptly, taking into account the notification requirements imposed on the Controller under the Applicable Privacy Laws, following the Processor's receipt of any inquiry from a Data Subject with respect to Controller Personal Data.

4.2.3 Provided that the Controller acts in accordance with Applicable Privacy Laws, the Processor shall not respond to any such request referred to in clause 4.2.2 unless expressly authorised to do so by the Controller.

4.3 **Regulatory action**: The Processor will promptly notify the Controller about:

4.3.1 any binding request addressed to the Processor or any of its Subprocessors for the disclosure of Controller Personal Data by a Regulatory Body unless otherwise prohibited by the applicable law; and

4.3.2 any monitoring activities and measures undertaken by the Regulatory Body, including where a Regulatory Body investigates the Processor for a possible breach of Applicable Privacy Laws.

4.4 **Audit rights**: The Controller has the right to, on reasonable notice and in a reasonable manner, audit and inspect the implemented technical and organisational security measures of the Processor and the Processor's compliance with this Agreement to the extent such measures are able to be audited. If the Processor notifies the Controller of a Personal Data Breach, then the Controller shall have the right to perform an on-site audit of the Processor on notice without undue delay. Any audit or inspection undertaken by the Controller shall be at the Controller's cost.

5 Personal Data Breach

5.1 **Data breach**: To the extent the Processor becomes aware of any Personal Data Breach or if it has reason to believe that a Personal Data Breach may have occurred, then the Processor must:

5.1.1 immediately notify the Controller, taking into account the notification duty requirements imposed on the Controller under the Applicable Privacy Laws; and

5.1.2 act immediately to:

(a) investigate the Personal Data Breach and no later than 24 hours after the Processor became aware of the Personal Data Breach, provide the Controller with the information set out in clause 5.2, or if it is not possible to provide all of that information within 24 hours then provide that information in phases without undue further delay; and

(b) with the prior consent of the Controller, take measures to prevent further Personal Data Breaches, and mitigate or remedy the Personal Data Breach.

5.2 **Information obligations**: The Processor shall summarise in reasonable detail the impact of the Personal Data Breach, including describing to the extent this is known to the Processor:

5.2.1 the nature of the Personal Data Breach;

5.2.2 the categories and numbers of Data Subjects concerned;

5.2.3 the categories and numbers of personal data records concerned;

5.2.4 the details of any unlawful recipient (including names, addresses and business sectors);

5.2.5 the estimated risk and the likely consequences of the Personal Data Breach; and

5.2.6 the measures taken or proposed to be taken to address the Personal Data Breach.

5.3 **Records**: The Processor shall maintain records of any actual or suspected Personal Data Breach in accordance with commercially accepted industry practices. The Processor shall make such records reasonably available to the Controller.

6 Technical and organisational security measures

6.1 **Confidentiality**: The Processor will:

6.1.1 ensure that the personnel it authorises to process Controller Personal Data are under appropriate confidentiality obligations; and

6.1.2 inform its authorised personnel that the Controller Personal Data is only to be processed as instructed by the Controller.

6.2 **Data Security**: During the processing of Controller Personal Data, the Processor shall take appropriate technical and organisational security measures to ensure a level of security appropriate to the risk of a Personal Data Breach.

6.3 **Security Measures**: Without limiting any such measures specified in the Terms of Service, the security measures adopted by the Processor include but are not limited to the following:

6.3.1 taking reasonable steps to ensure the reliability of any staff who have access to Controller Personal Data;

6.3.2 the encryption, and the pseudonymisation (where reasonably practicable) of Controller Personal Data;

6.3.3 ensuring the ongoing confidentiality, integrity, availability and resilience of the systems and services processing Controller Personal Data;

6.3.4 making best efforts to ensure it only stores Controller Personal Data on systems that meet or exceed its own security standards;

6.3.5 implementing a process for testing, assessing and evaluating the effectiveness of technical and organisational security measures for ensuring the security of the processing of Controller Personal Data; and

6.3.6 taking any other steps required by Applicable Privacy Laws.

7 Cross-Border Data Transfers

7.1 **Cross-Border Transfers**: Subject to clause 7.2, the Processor shall not transfer Controller Personal Data to a Third Country, except on written approval of the Controller (not to be unreasonably withheld or delayed), including as set out in the Terms of Service and this Agreement, and then subject to any additional restrictions reasonably required by the Controller or in compliance with Applicable Privacy Laws. The Controller shall not withhold consent in respect of any Subprocessor in a Third Country that the European Commission has recognised as providing adequate protection.

7.2 **Existing Transfers**: It is noted that the Processor is based in New Zealand and the Processor's Subprocessors are in Australia and Germany. The Controller acknowledges and agrees that:

7.2.1 the European Commission has recognised New Zealand, as providing adequate protection; and

7.2.2 except in respect of any Subprocessors existing at the date of this Agreement (to which consent of the Controller shall be deemed), it shall do so only by way of a:

(a) written agreement with the sub-processor which imposes similar obligations on the Subprocessor as are imposed on the Processor under this Agreement; and

(b) if required, the Standard Contractual Clauses.

The Controller explicitly grants the Processor a mandate to execute and enforce the Standard Contractual Clauses on its behalf against the Processor's relevant Subprocessors.

8 SubProcessors

8.1 **Subprocessors**: The Controller gives the Processor general written consent for the Processor to authorise any third party to process Controller Personal Data as a Subprocessor, subject to the following conditions:

8.1.1 the Processor must maintain an up-to-date list of the names and locations of all Subprocessors, and shall make this list reasonably available to the Controller. At the date of this Agreement, the only SubProcessor is Amazon Web Services, which is located in Germany; and

8.1.2 except in respect of any Subprocessors existing at the date of this Agreement (including Amazon Web Services), the contract entered into between the Processor and a Subprocessor will be on terms which are substantially the same as those set out in this Agreement, and will terminate automatically on expiration or termination of the Terms of Service.

The Processor will assume all liabilities for the acts and omissions of its Subprocessors in relation to the Services provided to the Controller.

9 LIABILITY

9.1 **Terms of Service**: Unless expressly prohibited by law, with regard to parties' liability to each other under or in connection with the Terms of Service and this Agreement, the provisions of the Terms of Service shall apply with respect to the parties' liability under this Agreement. To the extent permitted by law, any liability cap applicable to a party under the Terms of Service shall apply in respect of that party's total liability under this Agreement and the Terms of Service.

9.2 **Liability to Data Subjects**: Towards Data Subjects, the parties will be liable to the Data Subjects in accordance with article 82 of the GDPR (i.e. the Controller will be liable for the damage caused by processing which infringes Applicable Privacy Laws and the Processor will be liable for the damage caused by processing only where it has not complied with obligations of Applicable Privacy Laws specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Controller as provided for in this Agreement). Where one of the parties paid full compensation to the Data Subjects for the damage suffered, that party shall be entitled to claim back from the other party that part of the compensation corresponding to its part of responsibility for the damage (by way of a breach of any Applicable Privacy Laws or its obligations under the Terms of Service).

9.3 **Exclusion**: Neither party shall be liable to the other under this Agreement for any special, indirect or consequential loss or damages or liability for any direct or indirect: loss of profits, loss of revenue; loss of data (including any Controller Personal Data), loss of anticipated savings arising out of or in any way connected with these).

10 TERM AND TERMINATION

10.1 **Term**: This Agreement takes effect on and from the date it is signed by both parties and remains effective during the term of the Terms of Service.

10.2 **Termination**: Despite clause 10.1, the parties may terminate this Agreement earlier where both parties agree to terminate this Agreement in writing, or where the parties sign a new data processing agreement to replace this Agreement.

10.3 Return/Destruction of Controller Personal Data: Except as otherwise directed by the Controller, when requested to do so by the Controller the Processor shall hand over to the Controller all Controller Personal Data, and shall use all reasonable endeavours to erase or destroy related data as described in the Terms of Service.

11 NOTICES

11.1 All notification provided in this Agreement must be provided to the relevant contact details provided by each party in connection with the Terms of Service.

12 GENERAL

12.1 **Governing law and disputes**:

12.1.1 The clauses of this Agreement shall be governed by the law of the country in which the Controller is established.

12.1.2 The Processor agrees that if the Data Subject invokes against it third-party beneficiary rights and/or claims compensation for damages under this Agreement, the Processor will accept the decision of the Data Subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the country in which the Controller is established.

12.1.3 The parties agree that the choice made by the Data Subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

12.2 **Assignment**: Neither party may transfer, sell, or assign this agreement, or any of its rights, obligations or duties under, without the prior written consent of the other party, such consent not to be unreasonably withheld.

12.3 **Further assurances**: Each party will do all things and execute all documents reasonably required to give effect to the provisions and intent of this agreement.

12.4 **Relationship**: The relationship between the parties under this Agreement is that of customer and service provider and nothing expressed or implied in this Agreement constitutes either party or their personnel as the partner, employee or officer of, or as a joint venturer with, the other party

12.5 **Waiver**: No waiver of any breach, or failure to enforce any provision, of this Agreement at any time by either party will in any way affect, limit or waive that party's right to subsequently require strict compliance with this Agreement.

12.6 **Costs:** Each party shall cover its own costs incurred by it in connection with the negotiation, and execution of this Agreement.

12.7 **Amendments**: The parties undertake not to vary or modify the terms of this Agreement where mandated by the SCC. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the mandated terms.

12.8 **Terms of Service**: This Agreement is supplemental to (and forms part of) the Terms of Service, and other than as stated by this Agreement, the Terms of Service remain in full force and effect.

12.9 **Priority**: In the case of conflict or ambiguity between:

12.9.1 any of the provisions of this Agreement and the provisions of the Terms of Service, the provisions of this Agreement will prevail; and

12.9.2 any of the provisions of this Agreement and any executed SCC, the provisions of the executed SCC will prevail.

SCHEDULE A

EU STANDARD CONTRACTUAL CLAUSES

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……
(the data **exporter**)

And
Name of the data importing organisation:

Address:

Tel.: ; fax: ; e-mail:

Other information needed to identify the organisation:

……
(the data **importer**)
each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in 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[1];

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

  (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

  (ii) any accidental or unauthorised access, and

  (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely France

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely France.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……

(stamp of organisation)

On behalf of the data importer:
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature……

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
……
……
Data importer
The data importer is (please specify briefly activities relevant to the transfer):
……
……
Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
Reference is made to appendix B of the DPA

Categories of data
The personal data transferred concern the following categories of data (please specify):
Reference is made to appendix B of the DPA

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
Reference is made to appendix B of the DPA

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
Reference is made to appendix B of the DPA

DATA EXPORTER
Name:……
Authorised Signature ……

DATA IMPORTER
Name:……
Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.
Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Reference is made to appendix B of the DPA and the Terms of Service.

SCHEDULE 3 - BUSINESS ASSOCIATE AGREEMENT

BACKGROUND

D. You (the **Covered Entity**) and Noted Limited (the **Business Associate**) have entered into the Business Associate's Terms of Service for the provision of online services by the Business Associate for the Covered Entity.

E. The Covered Entity and the Business Associate have agreed to enter into this Agreement for the protection of the Protected Health Information that may be processed by the Business Associate in providing the Services. The Protected Health Information is confidential and requires special treatment and protection under the Privacy Rule, Security Rule and any amendments to those rules contained in the HITECH Act.

F. By this Agreement, the Business Associate agrees that any Protected Health Information it gains access to in connection with the Services must only be used or disclosed only in accordance with this Agreement, the Privacy Rule, the Security Rule and the Terms of Service.

AGREEMENT

1 Definitions

1.1 **Definitions**: Unless the context otherwise requires:

Agreement means this business associate agreement.

Breach means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted by the Privacy Rule which compromises the security or privacy of the Protected Health Information, as described in 45 C.F.R. 164.402.

CFR means the regulations promulgated under HIPPA as specified in the Code of Federal Regulations.

Business Day means a day other than a Saturday or Sunday or public holiday on which banks are open for commercial business in the country of the Business Associate.

Electronic Protected Health Information means individually identifiable health information that is transmitted or maintained by electronic media as described in HIPAA, and that the Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

HHS means the U.S. Department of Health and Human Services.

HIPPA means Health Insurance Portability and Accountability Act of 1996 (as amended by the HITECH Act), together with the CFR at Title 45, Part 160, Part 162 and Part 164, and other applicable laws.

HITECH Act means the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009.

Individual means the person who is the subject of the Protected Health Information, has the same meaning as the term "individual" as defined in HIPAA, and includes a personal representative in accordance with 45 C.F.R. 164.502(g).

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Covered Entity Personal Data.

Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information, C.F.R. at Title 45, Parts 160 and 164.

Protected Health Information has the same meaning as the term “protected health information” as described in HIPAA, limited to the information provided or made available by (or on behalf of) Covered Entity to the Business Associate.

Required by Law has the same meaning as the term “required by law” as defined in HIPAA.

Secretary means the Secretary of HHS or his or her designee.

Services means the services as described in the Terms of Service.

Security Rule means the Standards for the Security of Electronic Protected Health Information, C.F.R. at Title 45, Parts 160, 162 and 164.

Terms of Service means the Business Associate’s terms of service and its schedules, its Privacy Policy and any Letter of Agreement.

Unsecured Protected Health Information” has the same meaning as the term “Unsecured protected health information” as defined in 45 C.F.R. 164.402.

1.2 All other capitalised terms used in this Agreement shall have the meanings given to them in the Terms of Service.

1.3 **Interpretation**: In this Agreement where the context permits:

1.3.1 references to data subject, covered entity, business associate, identifiable, personal data, processing and special category personal data shall have the same meanings ascribed to them by the Applicable Privacy Laws;

1.3.2 reference to a party shall include that party's executors, administrators, successors and assigns;

1.3.3 reference to a statute or regulation shall include all amendments and re-enactments thereof;

1.3.4 writing includes electronic communications (including email) and written has a corresponding meaning; and

1.3.5 the clause headings are inserted for ease of reference only and do not affect the construction of this Agreement.

2 Permitted uses and disclosure by Business Associate

2.1 **Use and disclosure**: Subject to the terms of this Agreement, the Business Associate may use or disclose Protected Health Information:

2.1.1 to perform the Services and otherwise comply with its obligations under the Terms of Service and at law, provided that such use or disclosure complies with the Privacy Rule’s minimum necessary policies and does not violate the Privacy Rule or the Security Rule; and

2.1.2 for the proper management and administration of the Business Associate or to carry out Business Associate’s legal responsibilities, provided that:

(a) the disclosure is Required by Law; or

(b) the Business Associate obtains reasonable assurances from the person to whom the Protected Health Information is disclosed that the Protected Health Information will remain confidential and will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person.

2.2 **Limits on use and disclosure**: The Business Associate will not use or disclose any Protected Health Information for any purpose other than as expressly permitted or required by this Agreement or as Required by Law.

3 Business Associate obligations

3.1 **Appropriate safeguards**: The Business Associate will establish and maintain reasonable and appropriate administrative, physical, and technical safeguards to:

3.1.1 prevent the use or disclosure of the Protected Health Information, other than as permitted by this Agreement; and

3.1.2 protect the confidentiality, integrity, and availability of Electronic Protected Health Information.

3.2 **Reporting obligations**: The Business Associate will report to the Covered Entity any:

3.2.1 use or disclosure of Protected Health Information not provided for, or allowed by, this Agreement; and

3.2.2 security incidents regarding Electronic Protected Health Information of which Business Associate becomes aware.

3.3 **Subcontractors and agents**: The Business Associate will ensure that any agent, including a subcontractor, to whom Business Associate provides Protected Health Information agrees to:

3.3.1 the same restrictions and conditions that apply to Business Associate in this Agreement in respect of such Protected Health Information; and

3.3.2 implement reasonable and appropriate safeguards to protect any Electronic Protected Health Information.

3.4 **Right of access to information**: Subject to the terms of this Agreement, the Business Associate agrees to provide access to Protected Health Information in a Designated Record Set (if applicable) to the Covered Entity or, if directed by the Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. 164.524, at the written request of the Covered Entity.

3.5 **Amendments to information**: The Business Associate agrees to make any amendments to Protected Health Information in a Designated Record Set (if applicable), that the Covered Entity reasonably directs or agrees to pursuant to 45 C.F.R. 164.526, at the request of Covered Entity or an Individual, and in a reasonable time and manner.

3.6 **Access to records**: Subject to the terms of this Agreement, the Business Associate will make its internal policies, procedures, practices, books, and records relating to the use, disclosure, and safeguarding of Protected Health Information available to the Secretary or Covered Entity, in a reasonable time and manner, solely for purpose of the Secretary determining its compliance with the Privacy Rule and the Security Rule.

3.7 **Documenting disclosures**: The Business Associate will document disclosures of Protected Health Information (and other information directly related to such disclosures) as would be required for the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528.

3.8 **Supply of information**: Subject to the terms of this Agreement, the Business Associate will provide to the Covered Entity or relevant Individual, in a reasonable time and manner, the information referred to in clause 3.7, as necessary to permit the Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528.

3.9 **Mitigation**: The Business Associate will mitigate, to the extent reasonably practicable, any harmful effect that is known to the Business Associate of any breach by the Business Associate of this Agreement.

3.10 **Breach notification**: During the term of this Agreement, the Business Associate will notify the Covered Entity of any Breach, not later than 60 days after the Business Associate discovers such Breach (except in the case of a delay by law enforcement in accordance with 45 C.F.R. 164.412). The notification will include, to the extent possible, the identification of each Individual whose Unsecured Protected Health Information has

been, or is reasonably believed by the Business Associate to have been, accessed, acquired, used, or disclosed during the Breach, as well as any other information available to Business Associate that the Covered Entity is required to include in a notification to the Individual(s) under 45 C.F.R. 164.404(c).

4 Covered Entity obligations

4.1 **Notice requirements**: If required for compliance with the Privacy Rule, the Covered Entity will (in a reasonable and timely manner) provide the Business Associate with the notice of privacy practices that the Covered Entity produces in accordance with 45 C.F.R. 164.520, including any changes to such notice.

4.2 **Changes to authorisations**: The Covered Entity will (in a reasonable and timely manner), provide the Business Associate with written notice of any changes in, or revocation of, authorizations or permission by an Individual to use or disclose Protected Health Information, if such changes affect the Business Associate's permitted or required uses and disclosures.

4.3 **Restrictions**: The Covered Entity will (in a reasonable and timely manner) provide written notice to the Business Associate of any restrictions on the use or disclosure of Protected Health Information changing the Business Associate's obligations that Covered Entity has agreed to under 45 C.F.R. 164.522.

4.4 **Permissible requests**: The Covered Entity will not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule, the Security Rule, or this Agreement, if done by the Covered Entity.

5 Liability

5.1 **Terms of Service**: Unless expressly prohibited by law, with regard to parties' liability to each other under or in connection with the Terms of Service and this Agreement, the provisions of the Terms of Service shall apply with respect to the parties' liability under this Agreement. To the extent permitted by law, any liability cap applicable to a party under the Terms of Service shall apply in respect of that party's total liability under this Agreement and the Terms of Service.

5.2 **Exclusion**: Unless expressly prohibited by law, neither party shall be liable to the other under this Agreement for any special, indirect or consequential loss or damages or liability for any direct or indirect: loss of profits, loss of revenue; loss of data (including any Protected Health Information), loss of anticipated savings arising out of or in any way connected with these).

6 Term and termination

6.1 **Term**: This Agreement takes effect on and from the date it is signed by both parties and remains effective during the term of the Terms of Service.

6.2 **Termination**: Despite clause 6.1, the parties may terminate this Agreement earlier where both parties agree to terminate this Agreement in writing, or where the parties sign a new business associate agreement to replace this Agreement.

6.3 **Return/Destruction of Data**: Except as otherwise directed by the Covered Entity, when requested to do so by the Covered Entity the Business Associate shall hand over to the Covered Entity all Protected Health Information, and shall erase or destroy related data as described in the Terms of Service. The Business Associate shall retain no copies of the Protected Health Information.

7 Notices

7.1 All notification provided in this Agreement must be provided to the relevant contact details provided by each party in connection with the Terms of Service.

8 General

8.1 **Governing law**: This Agreement shall be governed by, and construed and enforced in accordance with, the laws of the United States of America.

8.2 **Assignment**: Neither party may transfer, sell, or assign this agreement, or any of its rights, obligations or duties under, without the prior written consent of the other party, such consent not to be unreasonably withheld.

8.3 **Further assurances**: Each party will do all things and execute all documents reasonably required to give effect to the provisions and intent of this agreement.

8.4 **Relationship**: The relationship between the parties under this Agreement is that of customer and service provider and nothing expressed or implied in this Agreement constitutes either party or their personnel as the partner, employee or officer of, or as a joint venturer with, the other party

8.5 **Waiver**: No waiver of any breach, or failure to enforce any provision, of this Agreement at any time by either party will in any way affect, limit or waive that party's right to subsequently require strict compliance with this Agreement.

8.6 **Costs:** Each party shall cover its own costs incurred by it in connection with the negotiation, and execution of this Agreement.

8.7 **Amendments**: Except as otherwise limited in this Agreement, the parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for the Covered Entity (and if applicable, the Business Associate) to comply with the requirements of the Privacy Rule, the Security Rule, and HIPAA. Otherwise, this Agreement may be amended in accordance with the Terms of Service.

8.8 **Terms of Service**: This Agreement is supplemental to (and forms part of) the Terms of Service, and other than as stated by this Agreement, the Terms of Service remain in full force and effect.

8.9 **Priority**: In the event of any conflict between the Terms of Service and this Agreement, the terms in this Agreement shall prevail (to the extent of any such inconsistency).