



GENERAL TERMS AND CONDITIONS OF SALE

ARTICLE 1: SCOPE OF THE TERMS AND CONDITIONS

The purpose of these general terms and conditions (the "**Terms**" or "**T&C's**") is to govern the contractual relations between Dental Monitoring, a *société par actions simplifiée* incorporated under the laws of France, having its registered office at 75, rue de Tocqueville, 75017 Paris, France ("**DM**") acting on its behalf and on behalf of its Affiliates, and you/your private practice (the "**Client**").

DM develops, manufactures and distributes software, digital infrastructures, protocols, interfaces, mobile applications (the "**Software Products and Services**") and hardware (the "**Hardware Products**") for use in the dental health sector (together the "**DM Solution**").

The Client is a dental practice providing dental and/or orthodontic services to patients.

The Client would like to provide the DM Solution to their patients.

Accordingly, the Terms and the related Data Protection Agreement are the commercial conditions which apply between DM and any Client and, therefore, the sole basis for commercial negotiations unless specific terms (such as a separate agreement) have been concluded with the Client. In which case the specific terms shall prevail over the Terms.

ARTICLE 2: DEFINITIONS

Capitalized terms set out below, including those in Article 1 of these Terms, shall have the following meaning:

- "**Affiliates**" means any entity controlled by DM. For the purpose hereof, the term "control" shall mean the power and authority to manage such an entity, whether directly or indirectly, through the holding of shares with a voting right, through a contract or otherwise.
- "**Agreement**" or "**T&C's**" or "**Terms**" means these terms and conditions of sale, including the Schedules, as it or they may be amended or supplemented from time to time, and the expressions "hereof", "herein", "hereto", "hereunder", "hereby" and similar expressions refer to this Agreement and to any particular Section or other portion of this Agreement.
- "**Business Account**" means the Client's account/dashboard on the platform DentalMonitoring ("**DM Platform**").
- "**Client**" has the meaning attributed to it in the Recitals.
- "**Confidential Information**" has the meaning attributed to it in Section 15.1.
- "**Customer Data**" has the meaning attributed to it in Section 9.
- "**Data Protection Agreement**" or "**DPA**" means the Data Protection Agreement attached to the Terms which must be accepted by the Client as part of the DM Solution.

- **“DM Solution”** has the meaning attributed to it in the Recitals. Details of the Software Products and Services and the Hardware Products included in the DM Solution are available on the Business Account.
- **“DM Customer Experience”** refers to the department of DM who manages the Clients’ requests including the Return and Refund requests.
- **“Documentation”** means all up to date manuals, instructions, specifications and other documents and materials, describing the features, components, or requirements of the DM Solution and which facilitate the use of the DM Solution that are provided to the Client under the Terms.
- **“Effective Date”** means the earlier of (i) the date on which the Client accepts the Terms, or (ii) the date on which the order form is signed.
- **“End User”** means any patient of the Client who is registered to use the DM Solution.
- **“Hardware Products”** has the meaning attributed to it in the Recitals and refers to the DM ScanBox with cheek retractors, the ScanBox Pro and Led Adapter.
- **“Hardware Warranty Policy”** describes (i) the conditions to return defective Hardware Products to DM (ii) how DM provides Clients with a Refund (iii) and the Hardware Warranty Process.
- **“Hardware Warranty Process”** refers to the path that must be followed by Clients to proceed with a Return of defective Hardware Products and get a Refund.
- **“Open-Source Components”** means any software component that is subject to an open-source copyright license agreement, including any Apache License, BSD License, GNU General Public License or GNU Library, or other obligation, restriction or license agreement that substantially conforms to the Open Source definition as prescribed by the Open Source Initiative.
- **“Parties”** means DM and the Client and **“Party”** means either of them.
- **“Personal Data”** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **“Refund”** refers to the possibility for Clients to obtain the reimbursement of their order by transfer on their bank account or credit note.
- **“Replacement”** or **“Replace”** refers to the possibility for Clients to get new Hardware Products.
- **“Return”** refers to the return of Hardware Products by a Client.
- **“Return and Refund Policy”** describes (i) the conditions to return to DM the Hardware Products (ii) how DM provides Clients with a Refund and (iii) the Return and Refund Process.
- **“Return and Refund Process”** refers to the path that must be followed by Clients to proceed with a Return of Hardware Products and get a Refund.
- **“Shop”** means the shop accessible on the DM Platform which allows Client purchase Hardware Products.
- **“Software Products and Services”** has the meaning attributed to it in the Recitals and refers to Monitoring, DM Engage, DM Insights, Smart STL.
- **“Technical and Maintenance Support”** means the technical and maintenance support described in Schedule A.
- **“Term”** means the period attributed to it in Section 13.1.

- **“Warranty Period”** refers to One (1) year from the date of the original purchase of the Hardware Products.
- **“Warranty Policy”** refers to the policy which describes the cases and conditions to get warranties from DM.

ARTICLE 3: FORMATION OF THE AGREEMENT

3.1. Formation of the Agreement, amendments and documentation.

The Client declares and guarantees to have the legal capacity to enter into this Agreement and, if they represent a company or any other organization having legal personality, to be authorized to act in the name and on behalf of this company or this organization.

Before start using Software Products and Service and/or purchasing Hardware Products on the Shop or directly *via* the DM’s customer service, the Client must (depending on the Client’s location) either :

- read, understand and electronically accept the Terms and the related Data Protection Agreement (the **“DPA”**) on the Business Account (by ticking the box provided for this purpose and, therefore, agree to comply with them). After accepting those, the Terms (including the DPA) remain available on the Business Account.

or

- read, understand and sign the order form (including the commercial terms and DM T&C’s) electronically or on paper.

The Terms may be amended by DM due to a legislative, regulatory, jurisprudential, technical amendment related to its business activity.

Any amendment shall be notified in advance to the Client and will take effect for any subsequent order or next billing period.

As a reminder : The Terms are applicable unless specific terms (such as a separate agreement) have been concluded with the Client. In which case the specific terms shall prevail over the Terms.

DM can decide to stop selling the DM Solution, totally or in part, at any time and shall inform the Client as soon as possible. In such a case, DM shall not be held liable.

3.2. Legal right of withdrawal

According to French law, the Client cannot claim the right of withdrawal due to DM’s field of activity.

Once the Agreement has been concluded, no cancellation, even partial, may be claimed by the Client, except in the case of force majeure as stated below in the Section 16.6.

ARTICLE 4: PRICING AND PAYMENT

4.1. Pricing

The pricing and currency are available either on the Business Account in (i) the "Billing" section via View Pricing list for the Software Products and Services pricing and in (ii) the “shop” section for the Hardware Products pricing or on the order form signed by the Client.

All prices are exclusive of any shipping costs, sales tax and any other applicable taxes as mentioned in section 16.7. The Client will bear shipping costs, all taxes, duties, bank charges in connection with the payment to be received by DM (such as any applicable withholding tax or sales tax, when applicable)

and other governmental charges resulting from this Agreement and the payment of any corresponding fees (the “**Taxes**”).

Subject to applicable prior notice requirements, DM reserves the right to increase and revise the applicable prices annually, at its sole discretion, including but not limited to adjustments for inflation, product developments, changes in insurance premiums, shipping costs and purchase prices, without requiring the Client’s prior approval. The updated prices shall apply as of the first month or billing period following the notification.

4.2. Invoicing and Payment terms

The Client shall pay DM invoices via the following payment methods :

- by bank card on the DM Platform;
- by bank transfer to Dental Monitoring bank account;
- by direct debit granted to Dental Monitoring.

The Client will be invoiced on a monthly basis for the Software Products and Services and at each order for the Hardware Products.

All the unpaid fees generated by the bank rejection of a settlement of the Client will remain at the financial expense of the latter.

Any invoices notifications shall be sent by DM to the email address provided by the Client on the Client’s account under “billing details”.

The invoices are available on the Business Account and invoice issuances are notified by email to the Client.

DM invoices shall be due and payable upon receipt, by the Client to DM. Banners can appear on the dashboard in case of overdue or pending invoices.

In the event of non-payment of any sums owed to DM on their due date, DM shall be automatically entitled, without any notice being required, to a late-payment penalty calculated at the biannual refinancing rate of the European Central Bank, applicable on January 1st or July 1st, increased by 10 points. DM shall also be entitled to damages, in accordance with applicable regulations, which amounts to 40 euros (Article D. 441-5 of the French Commercial Code) potentially increased by the recovery costs incurred and evidenced by DM (including, but not limited to, reasonable attorney’s fees) to collect any amount that is overdue.

In addition, DM reserves the right to suspend or cancel pending orders as well as suspend new patient creation until full payment is made and all amounts due along with the corresponding penalties without prejudice to any other remedies, and deactivate the Business Account within ten (10) days of a formal notice being sent.

If the incident that led to the deactivation procedure is not resolved, DM may delete the Business Account at the end of the notice period applicable to the case at issue.

In case of fraudulent use of the bank details or any kind of billing or payment issue, the Client is invited, as soon as the fraud is discovered or the issue is detected, to contact the billing teams at the following addresses :

- Europe : billing-eu@dental-monitoring.com
- North America : billing-na@dental-monitoring.com
- Australia & New Zealand : billing-au@dental-monitoring.com
- Asia : billing-hk@dental-monitoring.com
- UK : billing-uk@dental-monitoring.com

- Japan : billing-jp@dental-monitoring.com
- Other: billing@dental-monitoring.com

In addition, DM can modify the payment terms if the Client fails to pay a previous invoice. In such a case the amount shall be payable in full immediately.

4.3. Management and security of payments

Payment for the use of the Software Products and Services or purchase of Hardware Products is handled directly by DM.

For the payment by bank card, the management and the security of payments is ensured by Stripe.

The Client can read the legal documents of Stripe at this link: <https://stripe.com/en-fr/legal>.

For the payment by direct debit, the management and the security of payments is ensured by GoCardless.

The Client can read the legal documents of GoCardless at this link: <https://gocardless.com/legal/>.

ARTICLE 5: PROVIDING AND PERFORMANCE OF THE SOFTWARE PRODUCTS AND SERVICES

5.1. Access to the DM Solution

The conditions of access and use of the DM Solution are described in the terms and conditions of use available on the Client's Business Account.

5.2. Location

The Software Products and Services will be hosted on DM's servers.

5.3. Training

DM will provide training to the Client's staff on the DM Solution (subject to a virtual practice set up pack purchase).

5.4. Technical and Maintenance Support

Technical and Maintenance Support shall be provided by DM to the Client without any additional charge as set forth in Schedule A.

ARTICLE 6: DELIVERIES & WARRANTIES

6.1. Delivery of Hardware Products

6.1.1. Shipping

DM reserves the right to choose the appropriate method of delivery based upon Client's address.

6.1.2. Delivery time

The delivery time is approximate and provided for information.

DM undertakes to provide its best efforts to deliver the Hardware Products to the Client within the delay mentioned in the order but the effective delivery time may vary upon specific case.

In case of a specific request for packing or transport, the Client shall pay additional costs.

6.1.3. Warranty and return & refund policies for Hardware Products

DM has a Warranty Policy and a Return and Refund Policy described below.

6.1.3.1 Warranty Policy

Hardware Products sold by DM benefit from the statutory warranty against hidden defects, allowing Clients to return Hardware Products that are found to be non-compliant. This warranty covers only hidden defects existing prior to the purchase and affecting the normal use of the Hardware Products.

DM will also replace or refund any Hardware Product found to contain a manufacturing defect, including defects in materials or workmanship, provided that such defect is reported within the applicable Warranty Period. The Hardware Warranty applies solely to Clients who have purchased Hardware Products from DM. If the defect relates only to an accessory, DM shall replace the accessory only.

Notwithstanding the foregoing, DM shall remain liable for defective Hardware Products in the event of gross negligence or willful misconduct, in accordance with applicable law.

a. Requirements to be eligible for a Warranty

To be eligible for a Replacement or Refund, the warranty claim must be initiated (i) within two (2) years from the discovery of the hidden defect, for claims made under the statutory warranty against hidden defects, and (ii) within three (3) years from the date on which the Client became aware of the damage, provided that the claim is initiated no later than ten (10) years after the product was first placed on the market, for claims related to defective products.

Notwithstanding the foregoing, DM remains liable for damages resulting from defective products in cases of gross negligence or willful misconduct, in accordance with applicable law.

b. Exclusions

Software Products and Services are not covered by the Hardware Warranty Policy.

DM will not Replace and Refund Hardware Products that have been damaged either by Clients or their respective patients. This also includes any damage caused by the owner modifying, attempting to fix, or otherwise altering Hardware Products.

DM will not be liable to Replace or Refund any faulty Hardware Product that has been reported outside of the specified Warranty Period.

Furthermore, Hardware Warranty Policy does not cover damages caused to the Client's smartphone or any other personal effect that can be used with Hardware Products.

c. How to request the Warranty

The Client must send an email to : support@dental-monitoring.com to start the DM Hardware Warranty Process.

When sending their request, the Client must attach their invoice and provide the following information:

- An explanation of the Client's situation and their request;
- A phone number or an email address to contact the Client easily.

The DM Customer Experience will receive and review the Client's request and, if the Hardware Products comply with the above requirements, DM will send an email to the Client including all the steps that must be followed to return such Hardware Products and receive new ones in Replacement or to be Refunded.

Any missing information could lead to additional delays processing the Client's request.

The Client can count three-five (3-5 weeks) to be refunded on their bank account, from the reception of the email request if the Hardware Products comply with the above detailed requirements.

6.1.3.2 Return & Refund Policy

If the Hardware Products don't meet the Client's expectations, the Client can return the Hardware Products to DM within fourteen (14) calendar days from the delivery and receive a Refund as long as you comply with certain requirements.

The shipping costs are incurred by the Client, and are deducted from the Refund. Return costs are not reimbursed by DM.

Any Damaged, incomplete, or faulty Hardware Products may be covered by the Warranty Policy above.

a. Requirements to be eligible for a Return and Refund from DM

To be eligible for a Return and Refund the process must be started within fourteen (14) calendar days from the delivery and the Hardware Products must be:

- In its unopened, original, undamaged package and with all accessories.
- Unused.

Any Refund won't be granted to the Client if the Hardware Products don't comply with these requirements for any reason whatsoever.

b. Exclusions

Hardware Products purchased as part of a combined promotion package with Software Products and Services cannot be returned and refunded.

Software Products and Services are not refundable.

c. To Request a Refund

The Client must send an email to : support@dental-monitoring.com to start the DM Return and Refund Process.

When sending their request, the Client must attach their invoice and provide the following information:

- An explanation of the Client's situation and the Client's request;
- A phone number or an email address to contact the Client easily.

The DM Customer Experience team will receive and review the Client's request and, if the Hardware Products complies with the above requirements, DM will send an email to the Client including all the steps that must be followed to return the Hardware Products and receive a Refund.

Any missing information could lead to additional delays processing the Client's request.

The Client can expect three to five (3-5) weeks to be refunded to their bank account from receipt of the email request, if the Hardware Products meet the requirements detailed above.

DM only grants the Client with a Refund.

6.2. Provision of Software Products and Services

DM undertakes to provide its best efforts to provide the Software Products and Services to the Client

In the event of an incident resulting in the unavailability of the Software Products and Services, and if the merits of the complaint are recognized, DM can provide credits to the Client as described in Schedule A.

ARTICLE 7: RISKS TRANSFER & IMPORTATION

7.1 Risk transfer

The transfer of the ownership of the Hardware Products to the Client takes place upon invoicing to the Client.

7.2 Importation

Depending on applicable local laws and regulations, DM's entities established in each country assume and fulfill all importer responsibilities for sales made within the countries where DM operates.

Disclaimer – Applicable to Switzerland Only : for sales in Switzerland, as the legal manufacturer DM fully assumes and endorses all importer responsibilities on behalf of the clients, as outlined in Article 53, Section 3 of the Swiss Medical Devices Ordinance (MedDO, SR 812.213).

ARTICLE 8: INTELLECTUAL PROPERTY

8.1. Ownership

The DM Solution and the Documentation are the intellectual property of and are owned by DM. The structure, organization and code of the DM Solution are the valued trade secrets and confidential information of DM. The Client agrees that the DM Solution and the Documentation are licensed, as set forth below, not sold, to the Client by DM for use by the Client.

All rights not expressly granted are reserved by DM.

Neither the Client shall violate the intellectual property or any other rights of DM, including, without limitation, (i) copying or distributing DM learning videos or other materials or (ii) copying or distributing DM technology, unless it is released under Open-Source Licenses; (iii) using the word "Dental Mind", "Dental Monitoring", "Smile Mate", "Smile Simulation" or DM logos in any business name, email, or URL without the prior consent of DM.

Furthermore, during the Agreement, the Client shall:

- a) safeguard the DM Solution and the Documentation from infringement, misappropriation, theft, misuse or unauthorized access;
- b) assist DM, as DM may reasonably require it and at DM's expense, in maintaining the validity, enforceability and DM's ownership of the intellectual property rights in the DM Solution and the Documentation; and
- c) promptly notify DM in writing if the Client become aware of: (i) any actual or suspected infringement or other violation of DM's intellectual property rights in the DM Solution or the Documentation; or (ii) any claim that the DM Solution or the Documentation, in whole or in part, infringes, misappropriates or otherwise violates the intellectual property rights or other rights of any third party;
- d) fully cooperate with and assist DM in all reasonable ways in the conduct of any claim or action by DM to prevent any actual or threatened infringement, misappropriation or violation of DM's rights in the DM Solution and the Documentation.

8.2. License of the DM Solution

Subject to the payment of the Price, DM hereby grants to the Client a non-exclusive, non-sublicensable and non-transferable license to use the DM Solution in the Client's country pursuant to the Documentation as set forth in this Agreement.

The DM Solution includes certain Open-Source Components licensed under the terms set forth in each applicable license (each, an "Open-Source License").

DM reserves all rights attached to the DM Solution and the Documentation which are not expressly granted herein. The rights granted to the Client by the license are subject to the restrictions on use described below:

- a) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas or algorithms of any of the DM Solution, the Documentation or any other data related to the DM Solution;
- b) modify, translate, or create derivative works based on the DM Solution, the Documentation or any other data related to the DM Solution;
- c) copy, rent, lease, distribute, pledge, assign, or otherwise transfer or encumber any rights to the DM Solution or the Documentation;
- d) use the DM Solution in any manner that could damage, disable, overburden, impair or otherwise interfere with DM's provision of the DM Solution or the normal operation of the DM Solution;
- e) access the DM Solution for the purposes of monitoring availability, performance or functionality, or for any other benchmarking purposes, in any manner which materially interferes with the operation or performance of the DM Solution;
- f) create Internet "links" to the DM Solution or "frame" or "mirror" any content provided in the DM Solution on any other server, wireless or Internet-based device;
- g) attempt to obscure, mask or otherwise conceal any branding of, or relating to, the DM Solution in any way, including wrapping, enclosing or otherwise packaging the DM Solution inside another business application, system or process; and
- h) use or access the DM Solution to build or support and/or assist a third party in building or supporting other Hardware Products or Software Products and Services.

It is strictly forbidden for Clients to resell DM Software Products and Services and Hardware Products for any reason and by any means whatsoever to third parties without DM's prior approval.

ARTICLE 9: DATA AND PERSONAL DATA

The Client and End Users are and remain the owners of the data and Personal Data that they communicate via the DM Solution pursuant to this Agreement. Notwithstanding the foregoing, DM shall have the right to use the Client and End-User data for statistics purposes, to improve the DM Solution and to comply with regulations.

DM will treat any Personal Data of the Client and End Users, and any other related patient data (the "**Customer Data**") as confidential and use its best efforts to protect it from unauthorized third-party access (encryption, storage and use subject to current IT security standards).

DM will comply with all applicable data protection and privacy laws when accessing, collecting, processing, analyzing and otherwise using Customer Data, including the EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**") and local data protection regulations as for example HIPAA, UK Data Protection Act, PIPEDA, etc.

In connection with the use of the DM Solution by the Client, DM may have access to Personal Data as defined by GDPR. DM agrees to execute and comply with the Data Protection Agreement attached to the Terms and the Privacy Policy available on the Business Account.

ARTICLE 10: PROMOTIONAL MATERIALS

The Client is authorized to create and distribute promotional materials referring to the DM Solution using its own trademarks and logos, on any medium whatsoever, provided that these materials are established in accordance with DM's guidelines. In case of doubts regarding the compliance with DM's guidelines, the Client has the responsibility to contact DM for final approval (support@dental-monitoring.com). If not, the Client is taking the full and sole responsibility of the promotional material content.

The Client shall ensure that its promotional materials and other documents and information provided in connection with the DM Solution comply with applicable laws and regulations.

DM is authorized to mention its Clients on its website but also advertise Client usage of the DM Solution on its website and brochures. In such a case, DM commits to fulfill the potential Client's guidelines if any.

ARTICLE 11: REPRESENTATION AND WARRANTIES

11.1. Representations and warranties of both Parties

a) Authority

Each of the Parties represents and warrants to the other Party that it has the full right and authority to execute and deliver this Agreement and to perform its obligations under this Agreement, and that neither the execution nor delivery of this Agreement by such Party, nor consummation of the transactions contemplated hereby, will result in a breach or default under the terms and conditions of any contract, order, license, charter document or other agreement by which such Party is bound.

b) Organization

Each of the Parties represents and warrants to the other Party that it is a corporation duly organized, validly existing and in good standing under the laws of the jurisdiction of its incorporation and has all requisite power and authority to own, lease and operate its properties and to carry on its business as it is now being conducted.

11.2. Representations and warranties of DM

DM hereby represents and warrants to the Client that DM is the owner of the DM Solution or otherwise has the right to grant to the Client the rights set forth in this Agreement, including without limitation, any third party software, data and materials included in the DM Solution.

ARTICLE 12: RESPONSIBILITY & INDEMNITIES

12.1 Responsibilities of the Parties

a) Responsibility of DM

In general, DM is bound by an obligation of means towards the Client in the performance of the Terms.

DM shall not be liable for any delay or failure to perform the Terms justified by a breach by the Client of its obligations (such as failure to provide DM with the information necessary to perform the Terms) or by a case of force majeure.

DM shall not be liable for:

- Acts committed by third parties over which it has no control, or events directly attributable to the Client or End Users;
- Acts/damage suffered by the Client or End Users and caused by a case of force majeure or an event beyond DM's control;
- Acts that have caused indirect or unforeseeable damage to the Client or End Users.

The Client expressly agrees that DM shall only be liable for direct material damage, to the exclusion of any indirect damage.

The Parties agree to consider the following events as indirect damage: indirect or unforeseeable damage suffered by the Client or third parties, purely financial or commercial losses, loss of earnings, loss of profits or turnover, loss of use, unrealized savings, loss of business or customers, loss of opportunity, and loss of data.

In general, DM's liability is strictly limited to the services it performs directly and independently under these Terms from the Effective Date.

In any event, if DM's liability is recognized by a court of law, its liability shall be limited to the annual amount excluding tax of the service paid by the Client under these Terms.

b) Responsibility of the Client

The Client is responsible for its own actions, acts, and omissions that would constitute a breach of these Terms.

The Client is solely responsible for its use of the DM Solution and, in general, for all activities carried out via the DM Solution.

12.2 Indemnities

a) Intellectual Property Rights

DM shall defend, indemnify and hold harmless the Client, from any claims, liabilities or damages, arising in connection with any action or claim that the DM Solution infringes any intellectual property and/or proprietary right of a third party, provided that (i) the Client cooperates with DM's reasonable requests for assistance in the defense; and (ii) DM controls the defense, negotiation and settlement of any such claim; provided, that DM shall not settle or compromise any claim that would adversely affect the rights of the Client without the prior written consent of the Client, such consent not to be unreasonably withheld.

b) Exclusion

DM shall have no liability to the Client with respect to any claim of intellectual property rights infringement caused by (i) the Client's modifications to the DM Solution or combination of the DM Solution with non-DM hardware products; (ii) the Client's continued use of the infringing the DM Solution after having been notified of the alleged infringement; (iii) the Client's failure to use modifications to the DM Solution supplied by DM that would have avoided the infringement; or (iv) modifications made to the DM Solution by any person or entity other than DM.

c) Use of the DM Solution

The Client agrees to defend, indemnify and hold harmless DM and its affiliates, and each of their respective directors, officers, employees, contractors, agents and suppliers, from any claims, liabilities or damages, and related costs and expenses, arising out of or related to the Client's use of the DM Solution that is in breach of the Terms, provided that (i) DM cooperates with the Client's reasonable requests for assistance in the defense; and (ii) the Client controls the defense, negotiation and settlement of any such claim; provided, that the Client shall not settle or compromise any claim that would adversely affect the rights of DM without the prior written consent of DM, such consent not to be unreasonably withheld.

ARTICLE 13: TERM AND TERMINATION

13.1. Term of the Agreement

The Agreement commences at the Effective Date and the Client can stop using the DM Solution at any time. In such a case, termination shall be effective at the end of the current billing period.

13.2. Termination of Agreement

The Agreement may be terminated by either party if:

- a) The other Party becomes insolvent, is dissolved or liquidated, makes a general assignment of the benefits of its creditors, files or has filed against it a petition in bankruptcy, or has a receiver appointed for a substantial part of its assets;
- b) The other Party has committed a material breach (including but not limited to the default of payment of the fees pursuant to Section 3) and such breach has not been cured within 30 days of receipt of a written notice of such breach; or
- c) Any change in law or regulation that would: (i) make this Agreement or material portion of a party's performance under this Agreement illegal, or (ii) require that any material terms of this Agreement be extended to any non-Party.

13.3. Obligations upon Termination

Upon expiration or termination of this Agreement for any reason:

- a) the Client shall promptly cease representing, quoting, marketing or otherwise using the DM Solution;
- b) the Client shall promptly return to DM all copies of the Documentation or data originally provided by DM and which are the property of DM; and
- c) the Client shall pay all outstanding invoices or amounts owed to DM which shall become immediately due and payable on notice of termination.
- d) DM shall continue to provide the DM Solution to the Client and End-Users already registered to use the DM Solution for the length of the relevant treatment, subject to payment of the

corresponding fees by the Client, for a maximum period of 12 months following termination of the Agreement.

Termination and the foregoing remedies shall be in addition to, and not in lieu of, any other remedies that either Party may have at law or in equity and shall not relieve either Party of liability for any breach of contract occurring prior to the effective date of termination.

ARTICLE 14: NON- SOLICITATION

Until this Agreement is terminated, and for a period of one year following such termination, the Client shall not hire, employ, retain or solicit any person who is an employee, officer or director of DM. In case of non-compliance to this section, the Client may pay an amount of up to one (1) year of gross salary of the employee.

ARTICLE 15: CONFIDENTIALITY

15.1 Definition

In this Section, “**Confidential Information**” means all information that the disclosing Party designates as confidential or which ought to be considered as confidential from its nature or from the circumstances surrounding its disclosure, including without limitation all regulatory, commercial, financial, administrative, intellectual property and technological information of either Party and any information concerning this Agreement, but does not include information which:

- a) is known to the receiving Party before receipt from the other Party;
- b) is disclosed to the receiving Party in good faith by a third party who had a right to make such disclosure; or
- c) is made public by the disclosing Party, or is established to be a part of the public domain otherwise than as a consequence of a breach by the receiving Party of its obligations hereunder.

15.2. Limited Use

All Confidential Information of each Party shall be used by the other Party strictly and only for the purposes of this Agreement. Each Party agrees not to disclose to any third party any such Confidential Information without the written consent of the other Party or as required by court order.

15.3. Obligations of the Parties

Each Party shall have an obligation to prevent the other Party’s Confidential Information in its possession or control from being misappropriated, or wrongfully communicated by any employee, consultant or other person under the receiving Party’s control. If the receiving Party is required by a court or government authority to disclose Confidential Information, the receiving Party shall provide the disclosing Party with prompt notice, including the circumstances of such requirement, so that the disclosing Party may seek an appropriate protective order, and shall reasonably cooperate with the disclosing Party in an action by the disclosing Party to obtain an appropriate protective order. Upon termination of this Agreement, the Parties shall promptly return or destroy the other Party’s Confidential Information.

ARTICLE 16: MISCELLANEOUS

16.1. Entire Agreement

This Agreement contains the entire agreement and understanding of the Parties and shall supersede any prior agreements and understandings of the Parties with respect to the subject matter hereof.

16.2. Compliance with Laws and Severability

In the performance of its duties and obligations under this Agreement, each of the Parties shall at all times comply with all applicable laws. If any clause or provision of this Agreement is held to be invalid or unenforceable by any court of competent jurisdiction, the remainder of this Agreement shall not be affected thereby. All other clauses or provisions of this Agreement, not found invalid or unenforceable shall be and remain valid and enforceable.

16.3. Amendments and Captions

Terms may only be modified or amended in writing signed by duly authorized representatives of both Parties. The captions of this Agreement are for convenience and reference only and in no way define, limit or describe the scope of this Agreement or the intent of any provision hereof.

16.4. Notices

Any notice to be given by the Client to DM shall be in writing and shall be given by sending such notice by email to: support@dental-monitoring.com with a copy to legal@dental-monitoring.com.

16.5. Assignments

DM and the Client shall not assign this Agreement to a third party without prior written consent of the other Party. Each of the Parties shall have the right to assign this Agreement to its parent company, subsidiary or affiliated company. This Agreement shall be binding upon and shall inure to the benefit of the Parties hereto and their respective assigns as permitted under this Agreement.

16.6. Force Majeure

Neither Party shall be liable for any failure or delay in its performance under this Agreement due to causes of *force majeure*, including without limitation, fires, floods, storms, earthquakes, pandemics, civil disturbances, or labor matters, provided that the Client shall continue to be obligated to pay any fees that have accrued up until the event of *force majeure*. If a Party is so delayed or prevented from performing its obligations under this Agreement for a period of 30 consecutive days, the other Party shall have the immediate right to terminate this Agreement at the end of such 30 consecutive-day period, without any right of cure on the Party so delayed.

16.7. Taxes

The Client shall pay any taxes arising from this Agreement, including any customs duties and import taxes. DM is not responsible for any delays or additional costs resulting from customs processing.

16.8. No Waiver of Rights

No failure on the part of any Party to this Agreement to exercise, and no delay in exercising any right, power or single or partial exercise of any right, power or remedy by any Party shall preclude any other or further exercise thereof of the exercise of any other right, power or remedy.

16.9. Counterparts and delivery

This Agreement may be executed in several counterparts, each of which so executed shall be deemed to be an original, and such counterparts together shall constitute but one and the same instrument. Delivery of this Agreement by email shall constitute valid and effective delivery

16.10. Governing law and jurisdiction

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

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

SCHEDULE A

TECHNICAL AND MAINTENANCE SUPPORT

DEFINITIONS

- **“Error”** means a reproducible failure of the DM Solution to perform in substantial compliance with the specifications set forth in the Documentation, the origin of which can be isolated to a single cause.
- **“Incident”** means a request for support that begins when the Client provides DM with a Support Ticket with respect to one specific Error and ends when DM (i) Resolves the Error, or (ii) determines in its reasonable discretion that the Error cannot be resolved.
- **“Incident Backlog”**: means a list containing all the Errors that have been accepted by DM for which a solution has not yet been planned.
- **“Normal Business Hours”**: means Monday through Friday 9am – 6pm CET excluding bank holidays in France.
- **“Resolve/Resolution”** means the provision of (i) Technical and Maintenance Support that, in DM’s reasonable discretion, corrects the Error, (ii) information to the Client that corrects the Error, (iii) information to the Client on how to obtain a solution that corrects the Error, (iv) notice to the Client that the Error is caused by a known, unresolved issue or an incompatibility issue with the DM Solution, (v) information to the Client that identifies the Error as being corrected by an upgrade in the DM Solution, or (vi) notice to the Client that the Error has been identified as arising out of or resulting from an exclusion as set forth in Section 6 of this Schedule A.
- **“Respond/se”** means DM's initial communication with the Client, using the technical support e-mail or ticketing system provided by DM, acknowledging the Client’s requests for Technical and Maintenance Support in connection with a specific Error.
- **“Scheduled Maintenance Period”** means the maintenance periods scheduled by DM during which DM will cut off access to the DM Solution.
- **“Service Credit”** means the compensation granted by DM in case the availability of the DM Solution is not reached.
- **“Severity Level One Incident”** means an Error that causes an urgent and critical impact that impairs one or more major functions of the DM Solution, i.e. essential functions for the performance of the DM Solution. The Error shall have a critical impact on the Client’s business operations such that (i) it has affected or affects the entire user community, (ii) data integrity has been compromised, (iii) there has been a complete crash of the system, and/or (iv) it otherwise has caused an interruption of DM Solution’s major functions.
- **“Severity Level Two Incident”** means an Error which significantly affects material, but not essential aspects of the Client’s business operations, such that usage of the DM Solution can continue on a limited basis, but with a high risk to data integrity and/or significant interruption to critical processes.
- **“Severity Level Three Incident”** means an Error which does not substantially affect the Client’s normal business operations, including failures in software components that are non-critical.
- **“Severity Level Four Incident”** means an Error resulting in minimal or no interruptions to the Client’s normal business operations; this level includes primarily the Client inquiries, including questions pertaining to API’s, integrations, configuration, enhancement requests and Documentation.
- **“Support Ticket”** means the method to submit a request by the Client to the Technical and Maintenance Support.

1. SERVICES LEVEL OBJECTIVES

DM will use commercially reasonable efforts to make the DM Solution available and compliant with the performance objectives 99.9% of the time in any calendar month (the “**Monthly Uptime Percentage**”), except during the Scheduled Maintenance Period, in case of an exclusion as set forth in Section 6 of this Schedule A.

The Monthly Uptime Percentage is calculated by subtracting from 100% the percentage of continuous 5-minute periods during the service month in which the DM Solution was qualified as Unavailable Time.

“**Unavailable Time**” means any period during which the entire DM Solution (not only one of its features) is not available for use during the Client’s local opening hour (8:00 a.m to 6:00 p.m), provided however that DM Solution’s issues or outages relating to any exclusions as set forth in Section 5 of this Schedule A shall not be deemed as Unavailable Time.

Depending on the Monthly Uptime Percentage for each calendar month, as determined by DM, at its sole discretion, DM will apply a credit service the Client’s account with a percentage of such month’s billing, as follows:

Monthly Uptime Percentage	Service Credit
99.0% – < 99.9%	1 %
<99.0 %	5%

To qualify for a service credit, the Client must submit a written claim to DM within fifteen (15) calendar days following the end of the applicable month, including the necessary logs and supporting documentation. No service credit will be granted if the Client fails to meet this requirement.

The total amount of service credits granted to the Client in any twelve (12)-month period shall not exceed the equivalent of one (1) month of fees payable for the DM Solution. Service credits shall constitute the Client’s sole and exclusive remedy for any failure to meet the service levels described in this Schedule A.

2. TECHNICAL AND MAINTENANCE SUPPORT SCOPE

Subject to Terms and the Client’s and its End Users’ compliance therewith, during the Agreement, DM shall provide the following technical and maintenance support to the Client; provided, however, that DM shall not be held liable for any delay or failure to perform caused in whole or in part by any delay or failure to perform of the Client’s obligations under this Agreement or due to an exclusion as set forth in Section 5 of this Schedule A.

DM shall provide support in connection with Incidents, and the identification, diagnosis and Resolution of Errors, including: (i) e-mail assistance; (ii) remote troubleshooting services and analysis; and (iii) access to Documentation.

3. TECHNICAL AND MAINTENANCE SUPPORT RESPONSE TIME

During the Agreement, DM shall use commercially reasonable efforts to Respond to Incidents reported by the Client within the following timeframes:

- a) Severity Level One Incident: within two business hours from DM's receipt of the Client's Support Ticket for such Incident. In the event of a Severity Level One Incident, DM will make all commercially reasonable efforts to provide a temporary code patch as soon as practicable.
- b) Severity Level Two Incident: within four business hours of DM's receipt of the Client's Support Ticket for such Incident. A Severity Level Two Incident will be added to the Incident Backlog and assigned the highest priority for Resolution.
- c) Severity Level Three Incident: within one business day of DM's receipt of the Client's Support Ticket for such Incident. A Severity Level Three Incident will be added to the Incident Backlog and Resolved based on the relative severity and priority of outstanding Incidents, in the sole discretion of DM.
- d) Severity Level Four Incident: within two business days of DM's receipt of the Client's Support Ticket for such Incident. A Severity Level Four Incident will be added to the Incident Backlog and Resolved based on the relative severity and priority of outstanding Incidents, in the sole discretion of DM.

The Client acknowledges and agrees that, as part of the Incident support provided to the Client, DM may provide remote trouble shooting services to the Client to assist in analyzing and Resolving any Incident. The Client agrees to provide DM with the necessary access level to the Client's network, systems, and computers to install and use remote access software necessary for DM to provide such remote Incident support to the Client.

4. CHANGES TO TECHNICAL AND MAINTENANCE SUPPORT

DM may, in its sole discretion, change any aspect of the Technical and Maintenance Support or the performance thereof with thirty days' prior written notice to the Client, provided that no such change materially reduces or otherwise has a material adverse effect on the: (i) DM's obligation to provide the Technical and Maintenance Support under this Schedule; or (ii) the Client's rights under the Agreement or this Schedule.

DM may, in its reasonable discretion, perform any of the Technical and Maintenance Support by or through third parties or any of its affiliates.

5. EXCLUSIONS

DM has no obligation to provide Technical and Maintenance Support relating to Errors that, in whole or in part, arise out of or result from any of the following :

- a) any operation or use of, or other activity relating to, the DM Solution other than as specified in the Documentation, including any incorporation in the DM Solution of, or combination, operation or use of the DM Solution in or with, any technology (including any software, hardware, firmware, system or network) or service not specified for the Client's use in the Documentation, unless otherwise expressly permitted in writing by DM;
- b) any negligence, abuse, misapplication or misuse of the DM Solution;
- c) any delay or failure by the Client to perform any of the Client's obligations;

- d) any relocation, installation or integration of the DM Solution other than by the Client's personnel;
- e) any Open-Source Components, beta software, software use that DM makes available for testing or demonstration purposes, temporary software modules or software for which DM does not receive a license fee;
- f) the operation of, or access to, the Client system or network by a third party;
- g) any unavailable time or elevated latency time of the services provided by a cloud provider such as, but not limited to AWS, Microsoft Azure or Google Cloud;
- h) any breach of or noncompliance with any material provision hereof by the Client or any of their representatives;
- i) DM's suspension and termination of the Client's right to use the DM Solution in accordance with the Agreement; or
- j) any force majeure event (including abnormal physical or electrical stress).

6. LIMITATIONS

The Technical and Maintenance Support shall not include training of any kind with respect to the DM Solution.

DM will use commercially reasonable efforts to: (i) Respond within the applicable Response time provided herein; and (ii) Resolve an Incident, but does not guarantee that it will be able to Respond within such specific time period or that any Incident will be Resolved.

DM shall not be held liable for any delay or failure to perform caused in whole or in part by any delay or failure to perform of the Client's obligations under the Agreement.

7. CLIENT'S OBLIGATIONS

7.1. Notification

The Client shall promptly notify DM of any Error and provide DM with:

- a) specific details of the nature and circumstances of such Error;
- b) the Client perceived Incident severity level for such Error; and
- c) any information required by DM to reproduce such Error.

The Client shall provide the notification to DM by submitting a Support Ticket by emailing [it@dental-monitoring.com](mailto:it@ dental-monitoring.com).

The Client shall provide separate Support Tickets for each individual Error. An Error that can be divided into subordinate Errors shall be submitted on separate Support Tickets for each subordinate Error.

7.2. Equipment

The Client shall set up, maintain and operate in good repair and in accordance with the Documentation all necessary equipment, as well as all environmental conditions and components, including all networks, systems and hardware, in or through which: (i) the DM Solution operates; and/or (ii) the Client access or use any of the Technical and Maintenance Support.

7.3. Access

In connection with the performance of the Technical and Maintenance Support, the Client shall provide DM with all such cooperation and assistance as DM may reasonably request to enable DM to perform

its obligations including but not limited to, assisting DM with any installation, integration, regression and parallel testing of the DM Solution.

7.4. Information

The Client shall provide DM with all information reasonably requested by DM from time to time relating to the Client's use of the DM Solution, including information on Client's hardware, network, systems and any related third-party materials.

7.5. Data Back-up

The Client shall be responsible for regularly backing-up all data, files and information that they send to DM, as the DM Solution shall not be considered as a backup of the information provided by the Client.

7.6. Technical and Maintenance contact

The Client shall designate and maintain throughout the Agreement at most two individuals to serve as its primary point of contact for day-to-day communications, consultation and decision-making regarding the Technical and Maintenance Support (each, a "**Technical Contact**").

The Technical Contact(s) shall be the sole contact(s) between the Client and DM in connection with day-to-day matters relating to the provision of Technical and Maintenance Support and be responsible for reporting Incidents, providing day-to-day consents and approvals on behalf of the Client and communicating with and providing timely and accurate information and feedback to DM in connection with the Technical and Maintenance Support. The Client shall ensure its Technical Contact(s) have the requisite organizational authority, skill, experience and other qualifications to perform these duties. The Client shall use commercially reasonable efforts to maintain the same Technical Contact(s) in place throughout the Agreement and provide at least 30 days' prior written notice to DM of any replacement or change in the name or contact information of any Technical Contact.

7.7. Current Release

Except as otherwise agreed by DM in writing, the Client shall only run the current release level of the DM Solution that DM has made available to the Client. The Client shall install all maintenance releases as soon as reasonably possible but no more than 30 days from the date they are made available by DM, unless otherwise agreed with DM in writing.

DATA PROTECTION AGREEMENT

This Data Protection Agreement (the “**DPA**”) is entered into by and between Dental Monitoring SAS, incorporated under the laws of France, having its registered office at 75, rue de Tocqueville, 75017 Paris, France, acting on its behalf and on behalf of its Affiliates (“**DM**”) and you/your private practice (the “**Client**”).

RECITALS

WHEREAS, DM develops, manufactures and distributes software, digital infrastructures, protocols, interfaces, mobile applications and hardware for use in the dental health sector (the “**DM Solution**”).

WHEREAS, The Client is a dental practice which provides patients with dental and/or orthodontic services. The Client would like to provide patients with the DM Solution and, therefore, start using the DM Solution.

WHEREAS, this DPA is entered into between DM and the Client (each individually a “**Party**” and together the “**Parties**” as part of the Terms provided and accepted by the Client.

WHEREAS, one Party or both Parties are subject to Data Protection Laws, which requires that the relationships between the Parties be governed by a written agreement.

Pursuant to Data Protection Laws, this DPA describes the relations between two Joint Controllers which are :

- DM and the Client’s employer when the healthcare professional is employed by a third party entity; or,
- DM and the healthcare professional when the healthcare professional is self-employed (the “**Self-Employed HCP**”).

This DPA defines the role, capacity and liability of the Parties as detailed in [Appendix 1](#).

WHEREAS, the Parties wish to record the nature of the Processing operations in this DPA. Therefore, this DPA describes the purposes and means of Processing operations as detailed in DM’s Privacy Policy.

WHEREAS, this DPA only contains rules applicable to the Processing of Personal Data within the framework of the Terms, along with additional rules pertaining to the transfer of data outside of the EU/EEA, as may be applicable.

NOW, THEREFORE, in consideration of the obligations herein contained, the Parties have agreed that they shall Process any and all Personal Data on the terms set out in this DPA.

1. DEFINITIONS

For the purposes of this DPA:

- “**Affiliate**”: means an entity that owns or controls, is owned or controlled by or is under common control or ownership with another entity.

- “**Data Subject**”, “**Controller**”, “**Personal Data Breach**”, “**Processing**”, “**Processor**” and “**Supervisory Authority**” shall have the meaning assigned to them in Article 4 of the GDPR.
- “**Data Protection Laws**” means (i) the EU General Data Protection Regulation 2016/679 (“**GDPR**”), (ii) the e-Privacy Directive 2002/58/EC (“**e-Privacy Directive**”), and any further applicable legislation replacing the e-Privacy Directive and/or the GDPR; (iii) any data protection law, statute or regulation of a European Union (“**EU**”) Member State, which may apply to one of the Parties pursuant to its data Processing activities or its establishment within the EU and (iv) any guidelines or opinion adopted by the European Data Protection Board (“**EDPB**”) as to interpret the application of GDPR and the e-Privacy Directive (v) the decisions of the Supervisory Authority or the judicial or administrative courts of an EU Member State which are binding on one of the Parties by way of its data Processing activities or its establishment within the EU; and (vi) the decisions rulings adopted by the EUCJ or the ECHR regarding Personal Data and privacy protection and freedom of speech or freedom of information ;
- “**Personal Data**” shall have the meaning assigned to it in Article 4 of the GDPR, as applicable to the relevant Controller.

2. OBLIGATIONS OF THE PARTIES

Each Party undertakes to comply with the Data Protection Laws, as applicable to their activities and Processing.

Each Party warrants that it shall and shall procure that its employees, directors and agents (the “**Representatives**”) shall ensure the security, integrity and confidentiality of the Personal Data it processes in the context of the Terms.

The Parties shall maintain the records of all of their Processing activities (“**Processing Records**”). The Processing Records shall contain purposes of the Processing, categories of the Personal Data being Processed, sources of the Personal Data, recipients of the Personal Data, legal basis for the Processing activities, Personal Data retention periods resulting from the purposes of the Personal Data Processing or from applicable legal obligations, possible sharing of the Personal Data between the Parties, or the Personal Data remote access/availability by another Party or by a third party.

The Parties agree that Article 4 of this DPA describes in detail the Processing operation(s) in Appendix 1.

The Client has the responsibility of Joint Controller with DM for the data processing related to the health monitoring of their patients performed through the DM Solution as set out in Appendix 1. As such, the Client guarantees processing the Personal Data of the patients collected through the DM Solution in compliance with applicable Data Protection Laws. For any other data collected or processed by the Client during the course of the treatment and that are not shared with DM, the Parties acknowledge that they each act as a separate and independent controller so the Client will remain solely and fully responsible for compliance with applicable laws and regulations.

3. TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES

Each Party undertakes to and shall procure that its Representatives take the technical, organizational and structural measures necessary to ensure the security, integrity and confidentiality of the Personal Data it Processes as part of the Terms with a view to prevent any Personal Data Breach, in particular where the Processing involves the transmission of Personal Data over a network, notably:

- the destruction, alteration, misuse or loss of the Personal Data made accidentally or without authorization of the Controller;

- the disclosure of or access to the Personal Data in an accidental or non-authorized manner; or
- any form or purpose of Processing of the Personal Data which would be unlawful, unauthorized or not provided for in this DPA.

Security measures shall provide in particular that:

- premises where Personal Data is Processed are secured;
- authentication/identification mechanisms to access Personal Data on information systems are in place;
- a password policy is implemented and enforced;
- the network and the information systems are protected against intrusions and other attacks;
- backups of Personal Data are regularly performed; and
- the Representatives processing Personal Data are properly trained on data security, confidentiality and integrity measures.

4. OBLIGATIONS OF THE PARTIES ACTING AS JOINT CONTROLLER

4.1 Processing principles

When processing Personal Data as a Controller, each Party shall:

- process Personal Data fairly and lawfully;
- process Personal Data only for the purposes that are specified, legitimate and legally permissible by Data Protection Laws and not process Personal Data further in ways incompatible with such purposes;
- process Personal Data which is accurate, relevant and not excessive for the purposes for which it is collected and used and where necessary keep it up to date;
- adopt appropriate measures to retain Personal Data for no longer than is appropriate for the purposes for which it was collected, unless Personal Data is otherwise required to be kept by Data Protection Laws or other applicable laws;
- when notified of a change to Personal Data, update its records in accordance with the deadlines specified by Data Protection Laws;
- inform the Data Subject that his/her Personal Data is processed and provide him with all information required by Data Protection Laws;
- respect the rights of the Data Subjects pursuant to Data Protection Laws and handle the requests based on their rights appropriately; and
- process the special categories of Personal Data with additional care and consider seeking consent where required and implementing specific security measures.

4.2 Rights of Data Subjects

When acting as a Controller, each Party shall:

- provide in an intelligible form, upon written request from a Data Subject, the information that constitutes Personal Data processed by such Party in relation to the relevant Data Subject, and such supporting information as is required by Data Protection Laws, unless that Party is permitted by Data Protection Laws to refuse or only comply partially with the request. That Party may, where permitted by Data Protection Laws, charge a fee for the provision of copies of Personal Data requested by the Data Subject;

- take into account Data Subjects' legitimate interests and inform them of the logic involved with respect to decisions made using their Personal Data purely by automatic means with no human involvement and which (i) are intended to evaluate certain personal aspects relating to the individual ; and (ii) produce legal effects concerning the Data Subject or significantly affect him/her; and
- address the Data Subject's request within the timeline defined under Data Protection Laws.

Regarding the Data Subjects' requests to exercise their personal rights :

DM will be the designated point of contact for Data Subjects and will respond to Data Subject's requests related to the processing listed in Appendix 1.

Where the Client receives a Data Subject request related to the processing listed in Appendix 1 and for which both Parties are Joint Controllers, it will notify the request to DM within 3 days of receipt of the request and provide DM with all assistance, information and cooperation reasonably requested by DM to support in responding to (and, as appropriate, complying with) that Data Subject's request within the timescales prescribed by Data Protection Legislation. DM will also take such actions as are directed by the Client in responding to the Data Subject's request.

To do so DM shall :

- proceed with the ID confirmation of the Data Subject making such request as appropriate ; and then
- amend, update or delete, as appropriate or upon notification, any Personal Data which is found to be incorrect;
- comply with the Data Subjects' statutory right to object to the way their Personal Data is processed by such Party. All legitimate objections will be investigated and necessary action taken, including rectification, erasure or destruction of Personal Data, where appropriate.

4.3 Obligations required by Data Protection Laws or a Supervisory Authority

The Parties acting as Controllers shall share responsibility for performing, where applicable, at their own expense, any formality and procedure required by Data Protection Laws or a Supervisory Authority for the implementation of the Processing carried out by it or on its behalf.

The Parties shall fully cooperate to enable each Joint Controller to comply with Data Protection Laws or the requirements issued by a Supervisory Authority. In any case, the relevant Party receiving a request from a Supervisory Authority shall immediately inform the other Party, if possible in writing (by email).

The Client will be primarily responsible for any interactions with Supervisory Authorities in relation to the processing of jointly controlled Personal Data. If DM receives a communication from a Supervisory authority, it shall notify the Client immediately upon receipt of the request and shall provide the Client with all assistance, information and cooperation reasonably requested by the Client in connection with that communication. DM shall permit the Client to take the lead in determining how to respond to the Supervisory Authority's communication and will comply with the Client's reasonable instructions in dealing with that communication.

Each Party may share the Personal Data with a Supervisory Authority when:

- reasonably required in order to comply with Data Protection Laws, treaties or applicable international conventions and the request properly falls within the scope of such Supervisory Authority; or
- to establish, exercise or defend a legal claim or provide evidence (e.g. fraud, theft or report of suspected illegal activity).

To the extent permitted under Data Protection Laws, a Party may only disclose information to a Supervisory Authority provided that:

- such information relates to compliance with Data Protection Laws on the Processing of Personal Data for which it is acting as Joint Controller;
- the information does not contain any confidential information of other Parties or any of their respective Controllers or about or belonging to a third party;
- the information is not subject to the law of privilege or professional secrecy; and
- disclosure of the information would not be contrary to the other provisions of Data Protection Laws.

4.4 Data Breach Notification

Both Parties acting as Controller shall without undue delay, where feasible, no later than 72 hours after becoming aware of it, notify the other Party in writing (by email) of any Personal Data Breach relating to Personal Data Processed as part of the Terms, or breach of this DPA by itself, its Representatives or any third party of which it has knowledge or any other material event that may compromise the integrity, security or confidentiality of Personal Data, especially in case of theft, loss of the data support on which Personal Data has been disclosed or is retained, accidental deletion of Personal Data or in case of illegal or unauthorized access to Personal Data by a third party.

As part of that notification, the Party aware of the Personal Data Breach shall provide the other Party with : (i) a description of the nature of the Personal Data Breach, including the volume and type of Personal Data affected and the categories and approximate number of Data Subjects concerned; (ii) the likely consequences of the Personal Data Breach; and (iii) a description of the measures taken or proposed to be taken to address the Personal Data Breach including, where appropriate, measures to mitigate its possible adverse effects.

Each Party shall in a timely manner provide any reasonable cooperation and assistance requested by the other Party from time to time to enable both Parties to fulfill their obligations under the Data Protection Legislation.

5. CROSS-BORDER DATA TRANSFERS

Personal Data are stored on DM's local servers (AWS) depending on the country where the Client is located as follows :

- In the US :
 - Seattle
 - US East (North Virginia)
 - US West (Oregon)
- In Europe :
 - Frankfurt (Germany)

- Dublin (Ireland)
 - Paris (France)
- In Asia :
 - Tokyo (Japan)

In case of cross-border data transfer from inside to outside the EU/EEA (where applicable), the Parties acknowledge that if the level of protection granted by the country of the recipient is not adequate or, a minima, similar, Data Protection Laws require that specific measures and steps be taken to secure transfers of Personal Data.

In such a case, the Parties shall implement these additional measures in accordance with the Standard Contractual Clauses in the latest version adopted by the European Commission.

6. LIABILITY AND INDEMNIFICATION

Each Party represents and warrants to the other Party that it will indemnify and hold the other Party harmless against any loss and damage resulting from a breach by such Party or, its Representatives of its contractual obligations under this DPA and/or any applicable Data Protection Laws, including, but not limited to, loss of profits, reputation, image or business opportunity, and reasonable documented attorney's fees to the extent of and subject to potential limitation of liability agreed between the Parties.

Both Parties, acting as Joint Controllers, shall be liable for the damages caused to third parties by Processing which infringes applicable Data Protection Laws.

7. MISCELLANEOUS

7.1. Termination

The DPA shall automatically terminate upon termination or expiry of the Terms for any reason, notwithstanding the survival of applicable provisions for as long as Personal Data related to a Party is retrained by the other Party.

7.2. Entire Agreement

This DPA shall supersede any prior agreements and understandings of the Parties with respect to its subject matter hereof and, in particular, over any particular provisions as part of the Terms which may have been related to the Processing of Personal Data.

7.3. Governing law and venue

This DPA and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and constructed in accordance with the laws determined in the Terms of Sale accepted by the Client as part of the Dental Monitoring Subscription.

Each Party irrevocably agrees that the courts determined in the Terms of Sale accepted by the Client as part of the Terms shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this DPA or its subject matter or formation.

APPENDIX 1

DETAIL OF THE PROCESSING

Processing	Description of Processing operation	Role of DM	Role of Client	Categories of Personal Data Involved
MANAGEMENT OF ACCOUNT				
Management of Client's account and End User account	Account's creation; account's configuration on DM solution; account's modification; account's deletion	Controller	Controller	- Account Data - Technical Data - Usage data
TECHNICAL AND MAINTENANCE SUPPORT				
Management of technical and maintenance support for Client	Support in connection with Incidents, and the identification, diagnosis and Resolution of Errors as detailed in the Technical and Maintenance Support in Schedule C	Controller		- Account data - Technical data - Usage data - Support ticket data
Management of technical and maintenance support for End Users	Customer support contact; creation of support ticket; exchanges with DM customer support; resolution of issue	Controller		- Account data - Support ticket data
PROVISION OF THE DM SOLUTION				
Management of contractual relationship	Negotiation and execution of Agreement; subscription to DM Solution; orders and deliveries of DM Solution; billing.	Controller		- Contact data - Subscription data

Monitoring of End User's health (establishment and validation of reports of End Users)	Creation and validation of health reports to suggest treatments options; Remotely monitoring of the patient's treatment performed by Client's Practices through DM Solution	Controller	Controller	• Medical data • Account data
Research and Development activities	Carrying out of research and development activities to improve the performance of DM neural networks used to analyze the scans.	Controller		• Medical data (pseudonymized) • Account data
Optimization of DM Solution	Ensure the security, confidentiality, integrity and availability of DM Solution; improve DM Solution and develop new features	Controller		• Account data • Technical data • Usage data
MANAGEMENT OF PRIVACY RIGHTS				
Management of Customers Data's rights	Client's employees, End user rights to access, rectification, erasure, restriction, objection, data portability their Personal Data processed by DM	Controller	Controller (<i>case by case basis</i>)	• Account data • Technical data • Usage data • Support ticket data • Subscription data • Medical data

APPENDIX 2

TECHNICAL AND SECURITY MEASURES

General Measures

DM implements technical and organizational measures to reduce risks inherent to Personal Data Processing:

- DM Representatives are trained on cybersecurity with a focus on data security, confidentiality and integrity measures;
- Information security policies are implemented and enforced throughout the company;
- DM conducts regular penetration tests on its infrastructure.

Access Control

DM implements measures to ensure that physical access to premises where Personal Data is Processed is controlled and secured:

- All DM Representatives are provided with an individual keycard to access the premises;
- DM Representatives Processing Personal Data are segregated in the premises;
- A visitor policy is enforced to ensure access to the premises for visitors is limited.

DM implements measures to control access to Personal Data:

- Access to networking infrastructure is restricted and controlled;
- Privileged access rights to systems are restricted and controlled;
- Individual credentials are required to access DM Solution;
- Access to Personal Data in DM's systems shall be further restricted through user roles.

Encryption

DM encrypts Personal Data in transit and data at rest:

- At rest: AES-XTS-256 ;
- In transit: TLS 1.2.

Hosting

DM products' infrastructure and Personal Data storage are hosted in the cloud. DM provider's cloud services are ISO 27001 certified, GDPR and HIPAA compliant.

BUSINESS ASSOCIATE AGREEMENT

This business associate subcontractor agreement (the “**Business Associate Agreement**”) is entered into by and between Dental Monitoring America Inc., a corporation incorporated under the laws of Delaware, having offices at Suite Number 140, 9500 Arboretum Boulevard, Austin TX 78759 (USA)(“DM”) and you/your private practice (the “**Client**”).

RECITALS

WHEREAS, Congress enacted the Health Insurance Portability and Accountability Act of 1996 (“**HIPAA**”) and the Health Information Technology for Economic and Clinical Health Act (“**HITECH**”), which provides protection for Protected Health Information.

WHEREAS, pursuant to HIPAA and HITECH, the United States Department of Health and Human Services (“**DHHS**”) promulgated HIPAA Regulations governing the privacy and security of certain health information as set forth in 45 CFR Parts 160 and 164.

WHEREAS, the Client is a Covered Entity which requires that if the Client provides Protected Health Information to any subcontractor or agent of the Client, then the Client must put in place a business associate agreement (“**BAA**”) with such subcontractor or agent .

WHEREAS, DM develops, manufactures and distributes software, digital infrastructures, protocols, interfaces, mobile applications and hardware for use in the dental health sector (the “**DM Solution**”).

WHEREAS, The Client is a dental practice which provides patients (“**Individuals**”) with dental and/or orthodontic services. The Client would like to provide Individuals with the DM Solution and, therefore, subscribe to the DM Solution ((the “**DM Solution Subscription**”).

WHEREAS, DM is performing certain functions on behalf of the Client under which the Client may disclose to DM, or DM may have access to, receive, create, maintain, or transmit, Protected Health Information on behalf of the Client requiring the Client to enter into a BAA with DM in connection with the DM Solution Subscription.

NOW, THEREFORE, in consideration of the foregoing recitals, the mutual promises and covenants set forth herein and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

1. DEFINITIONS

- “**Business Associate**” has the same meaning as the term "business associate" in 45 CFR § 160.103, and in reference to this Business Associate Agreement, shall mean DM.
- “**Covered Entity**” has the same meaning as the term “covered entity” in 45 CFR 160.103, limited to the entity or entities who have entered into a business associate agreement with the Client.

- **“Disclosure”** means the release, transfer, provision of, access to, or divulging in any other manner of Protected Health Information outside the entity holding such information.
- **“Electronic Protected Health Information”** has the same meaning as the term “electronic protected health information” in 45 CFR § 160.103, limited to the Covered Entity’s information created or received by DM from or on behalf of the Client or the Covered Entity.
- **“Individual”** means the person who is the subject of Protected Health Information, as defined herein, that DM is provided with, receives or otherwise obtains in connection with the performance of its obligations under the DM Solution Subscription made by the Client.
- **“HIPAA Regulations”** means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
- **“Protected Health Information”** has the same meaning as the term “protected health information” in 45 C.F.R. § 160.103 and means information, including demographic information, that (1) relates to (i) a past, present, or future physical or mental health or condition; (ii) the past, present, or future provision of health care; or (iii) the past, present, or future payment for the provision of health care; and (2) identifies the person who is the subject of the information or with respect to which there is a reasonable basis to believe the information can be used to identify such person. Protected Health Information is limited to the Covered Entity’s information created or received by DM from or on behalf of the Client or the Covered Entity.
- **“Required by Law”** means a mandate contained in law that compels an entity to make a use or disclosure of Protected Health Information and that is enforceable in a court of law as provided in 45 CFR § 164.103.
- **“Secretary”** means the Secretary of the U.S. Department of Health and Human Services or his or her designee.
- **“Security Incident”** has the same meaning as the term “security incident” in 45 CFR § 164.304.
- **“Unsecured Protected Health Information”** has the same meaning as the term “unsecured protected health information” in 45 CFR § 164.402, limited to the Covered Entity’s information created or received by the Client or on behalf of the Client or the Covered Entity.

Terms used in this Business Associate Agreement but not otherwise defined herein shall, if they are defined in the HIPAA Regulations, have the meanings attributed to them in those regulations.

2. OBLIGATIONS OF DM

2.1. Use and Disclosure of Protected Health Information

DM agrees that it shall create, receive, use, disclose, transmit and maintain all Protected Health Information disclosed to it by the Client in accordance with the terms and conditions of this Business Associate Agreement or as Required by Law provided, however:

- DM will not be permitted to use or disclose Protected Health Information in any manner which would violate the HIPAA Regulations if used or disclosed by a Covered Entity;

- DM shall not sell Protected Health Information or receive any direct or indirect remuneration in exchange for Protected Health Information.

2.2. Other Permitted Uses and Disclosures

- a) Except as otherwise prohibited by this Business Associate Agreement, DM may use Protected Health Information it receives, creates, maintains, or transmits:
 - to comply with applicable laws; or
 - for statistics purposes and/or to improve products developed by DM.
- b) Except as otherwise prohibited by this Business Associate Agreement, DM may disclose to a third party Protected Health Information it receives or creates for or on behalf of the Client for the proper management and administration of DM, provided that:
 - the disclosure is Required by Law, or
 - DM obtains reasonable assurances from the third party to whom the information is disclosed that (i) 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 third party, and (ii) the third party notifies DM of any instances of which it is aware in which the confidentiality of the information has been breached.

2.3. Establishment of safeguards

DM shall use and implement appropriate safeguards to prevent any use or disclosure of Protected Health Information other than as provided by this Business Associate Agreement and comply with Subpart C of 45 CFR Part 164 and to protect the confidentiality, integrity and availability of the Protected Health Information.

2.4. Use by Agents and Subcontractors

DM may disclose Protected Health Information created for or received from or on behalf of the Client or a Covered Entity only to the extent expressly permitted by the DM Solution Subscription or upon the prior written consent of the Client. DM agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information created or received by DM on behalf of the Client or the Covered Entity, agrees to the same restrictions and conditions that apply to DM through this Business Associate Agreement with respect to that information. The Business Associate will ensure only those who reasonably need to know such information in order to provide services related to the DM Solution Subscription receive such information and, in such case, consistent with the Minimum Necessary standard under the HIPAA Regulations.

2.5. Reporting of Illegal, Unauthorized or Improper Uses or Disclosures and Remedial Actions

DM shall notify the Client upon becoming aware of the following:

- any use or disclosure of Protected Health Information by DM not permitted by this Business Associate Agreement; or

- any material Security Incident affecting Electronic Protected Health Information created, received, maintained, or transmitted by DM on behalf of the Client or the Covered Entity.

2.6. Books and Records

DM shall make its internal practices, books and records, if any, relating to the use and disclosure of (a) Protected Health Information received from, or created or received by DM on behalf of the Client or the Covered Entity, and (b) Electronic Protected Health Information created, received, maintained or transmitted by DM on behalf of the Client or the Covered Entity, available to the Client and the Secretary as necessary to satisfy covered entity's obligations under 45 CFR 164.524.

2.7. Access to Protected Health Information

In the unlikely event an Individual seeks access to his or her Protected Health Information contained in a Designated Record Set and that Protected Health Information is in the possession or control of DM, and the Client notifies DM of the Individual's request, DM agrees to provide the relevant Protected Health Information to the Client within ten (10) business days of notice from the Client so that a Covered Entity may comply with the procedures set forth in 45 CFR §164.524.

DM will provide such Protected Health Information in an electronic format upon request by the Client.

2.8. Amendments to Protected Health Information

The Client shall notify DM within ten (10) business days of making an amendment to an Individual's Protected Health Information contained in a designated record set that is held by DM.

DM agrees to amend Protected Health Information in its possession at the direction of the Client within ten (10) business days of notice from the Client and upon the Client's request and at the Client's expense, to transmit or send to the Client a copy of the amended Protected Health Information within ten (10) business days thereafter.

2.9. Accounting of Disclosures

In the unlikely event that DM makes a disclosure subject to the requirements set forth in this Section 2.9, DM shall document its disclosure of Protected Health Information and information related to such disclosure as would be required for a Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528.

Within twenty (20) business days of a request by the Client, DM shall provide the Client with an accounting of all information collected in accordance with Section 2.9 of this Business Associate Agreement by DM during the previous six (6) years, in order for a Covered Entity to comply with its obligations under 45 CFR §164.528 to provide Individuals with an accounting of disclosures.

2.10. Amendment to Comply with the HIPAA Regulations

In the event HIPAA, HITECH, or the HIPAA Regulations are amended or, in the opinion of the Client's counsel, interpreted to require changes in the obligations of the parties under this Business Associate Agreement, the parties hereto agree to amend this Business Associate Agreement, or enter into a new agreement to come into compliance with such change. If it is determined by the Client's counsel that either the Agreement or this Business Associate Agreement is not in compliance with the HIPAA

Regulations, the parties hereto agree that they will amend such agreements, or enter into new agreements, as necessary, to comply with the HIPAA Regulations.

2.11. Compliance With HIPAA

DM agrees to comply with Sections 164.308, 164.310, 164.312 and 164.316 of title 45, Code of Federal Regulations. Furthermore, DM agrees to comply with all other applicable rules and regulations adopted pursuant to HIPAA and HITECH, including, without limitation, applicable provisions of the HIPAA Regulations, as such may be in effect and amended from time to time.

2.12. Property Rights

DM acknowledges that Protected Health Information shall be, and remain at all times, the property of a Covered Entity and DM shall acquire no title or rights to Protected Health Information as a result of this Business Associate Agreement.

2.13. Breach Notification

DM, following the discovery of a Breach of Unsecured Protected Health Information, shall notify the Client of such Breach. Except as otherwise required by law, DM shall provide such notice without unreasonable delay, but in no case later than five (5) business days, after DM has Knowledge (as defined under the HIPAA Regulations) of the Breach.

Notice to the Client required by this Section 2.13 shall include: (i) to the extent possible, the names of the Individual(s) whose Unsecured Protected Health Information has been, or is reasonably believed by DM to have been accessed, acquired, used or disclosed during the Breach; (ii) a brief description of what happened including the date of the Breach and the date of the discovery of the Breach, if known; (iii) a description of the types of Unsecured Protected Health Information that were involved in the Breach; (iv) a brief description of what DM is doing or will be doing to investigate the Breach, to mitigate harm to the Individual(s), and to protect against further Breaches; and (v) any other information that the Client or a Covered Entity determines it needs to include in notifications to the Individual(s) under 45 CFR § 164.404(c).

After receipt of notice, from any source, of a Breach involving Unsecured Protected Health Information used, disclosed, maintained, or otherwise possessed by DM, or of a Breach involving Unsecured Protected Health Information for which DM is otherwise responsible, the Client may (i) request that DM use a mutually agreed upon written notice to notify, on the Client's or a Covered Entity's behalf, the Individual(s) affected by the Breach, in accordance with the notification requirements set forth in 45 CFR

§ 164.404, without unreasonable delay, but in no case later than sixty (60) days after DM has Knowledge of the Breach; or (ii) elect to provide notice to the Individual(s) affected by the Breach. DM shall indemnify, hold harmless, and defend the Client and Covered Entity from and against any and all reasonable documented costs, losses, penalties, fines, and liabilities arising from or associated with the Breach, including without limitation the costs of the Client's or Covered Entity's actions taken to (i) investigate the Breach, (ii) notify the affected Individual(s) of and to respond to the Breach, (iii) mitigate harm to the affected Individual(s), and (iv) respond to questions or requests for information about the Breach.

3. OBLIGATIONS OF THE CLIENT

3.1. Notice of Restrictions on Use or Disclosure

The Client shall notify DM of any limitations (i) to which it has agreed in accordance with 45 CFR § 164.522; or (ii) imposed by the Individual, all to the extent that such limitation may affect DM's use or disclosure of Protected Health Information.

3.2. Permissible Requests by the Client

The Client shall not request DM to use or disclose Protected Health Information in any manner that would not be permissible under the HIPAA Regulations if done by a Covered Entity.

4. TERM AND TERMINATION

4.1. Term of Business Associate Agreement

The initial term of this Business Associate Agreement shall be the same as the term of the DM Solution Subscription. This Business Associate Agreement shall continue until all of the Protected Health Information provided by the Client or Covered Entity to DM, or created or received by DM on behalf of the Client or the Covered Entity, is returned to the Client, or, upon prior written approval of the Client, destroyed. If it is infeasible to return or destroy the Protected Health Information, then DM shall extend protections to such information as set forth in the termination provisions in Section 4.3.

4.2. Termination of the Business Associate Agreement

The Client shall have the right to terminate this Business Associate Agreement in the event of a material violation by DM of its obligations hereunder in order for the Client or a Covered Entity to maintain compliance with HIPAA, if DM fails to cure such material violation within thirty (30) calendar days of receiving notice thereof from the Client. However, in the event that the default cannot be cured within the thirty (30) day cure period, the thirty (30) day cure period may, in the sole discretion of the Client, be extended for a reasonable additional time to cure such default, provided that: (i) DM commences to cure the default within the thirty (30) day cure period, and (ii) proceeds diligently to effect the cure within such reasonable additional time. Notwithstanding the foregoing, if DM materially violates this Business Associate Agreement and cure is not possible, as determined by the Client, the Client may immediately terminate this Business Associate Agreement.

4.3. Obligations upon termination

Upon termination of this Business Associate Agreement, DM shall return or destroy all Protected Health Information received from the Client (or created or received by the Client on behalf of DM or the Covered Entity) that DM still maintains in any form and retain no copies of such Protected Health Information, to the exception of information retained in DM's standard computer back-up systems pursuant to DM's normal document and e-mail retention policy.

In the event DM determines that returning or destroying Protected Health Information is not feasible, DM shall extend the protections of this Business Associate Agreement to such Protected Health Information and shall limit further use and disclosure of such Protected Health Information, for so long as DM maintains such Protected Health Information.

If DM destroys Protected Health Information, it shall certify to the Client in writing that such Protected Health Information has been destroyed. Destruction of Protected Health Information must be in accordance with the HIPAA Regulations and guidance of the Secretary on and processes for ensuring that reconstruction, re-use, and/or re-disclosure of Protected Health Information is prevented after destruction

with the exact method of destruction dependent upon the media in which Protected Health Information is contained.

DM shall cooperate with the Client to ensure the return or destruction of Protected Health Information held by subcontractors or agents of DM.

5. MISCELLANEOUS

5.1. Compliance with Laws and Severability

DM agrees to comply with all applicable federal and state laws for the protection of personal information and the reporting of security breaches.

If any portion or portions of this Business Associate Agreement shall be, for any reason, invalid or unenforceable, the remaining portion or portions shall nevertheless be valid, enforceable and carried into effect, unless to do so would clearly violate the present legal and valid intention of the parties hereto.

5.2. Notice

Any notice to be given by the client to DM shall be in writing and shall be given by sending such notice by email confirmed to : legal@ dental-monitoring.com.

5.3. Subpoenas, Court Orders, and Governmental

If DM receives a court order, subpoena, or governmental request for documents or other information containing Protected Health Information, DM will use its best efforts, to the extent permitted by applicable laws, to notify to the Client the receipt of such request within five business days and to provide the Client with an opportunity to respond.

5.4. Governing Law

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

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

5.5. No third-party beneficiaries

This Business Associate Agreement is for the sole and exclusive benefit of the parties hereto and is not intended to, nor does it, confer any benefit upon any third party.

5.6. Counterparts and delivery

This Business Associate Agreement may be executed in several counterparts, each of which so executed shall be deemed to be an original, and such counterparts together shall constitute but one and the same instrument. Delivery of this Agreement by email shall constitute valid and effective delivery.