

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the “Agreement”) is effective as of _____ (the “Agreement Effective Date”) by and between Maimonides Medical Center located at 4802 Tenth Avenue, Brooklyn, New York 11219, and/or its affiliated entities Infusion Options, Inc., MMC Pharmacy, Inc., and/or any of its affiliated faculty practices, as applicable (collectively, “CE”) and _____, located at _____ (“BA”).

RECITALS

WHEREAS, CE has engaged BA or intends to engage BA to provide _____ (the “Services”) and/or other services not specifically described herein. The Services may be further described in a separate writing (the “Underlying Agreement”); and

WHEREAS, CE possesses Protected Health Information (as hereinafter defined) and is permitted to use or disclose such information only in accordance with HIPAA; and

WHEREAS, BA may receive such information from CE, or create, receive, maintain or transmit such information on behalf of CE, in order to perform certain functions and services or provide goods or both; and

WHEREAS, CE wishes to ensure that BA will appropriately safeguard Protected Health Information;

NOW THEREFORE, CE and BA agree as follows:

- I. **Definitions.** The parties agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in HIPAA.
- A. “*HIPAA*” means the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, incorporated in the American Recovery and Reinvestment Act of 2009 and the Privacy, Security, Breach Notification, and Enforcement Regulations at 45 C.F.R. Part 160 and 45 C.F.R. Part 164.
 - B. “*Breach*” shall mean the unauthorized acquisition, access, use, or disclosure of Unsecured Protected Health Information which compromises the security or privacy of such information, as set forth in 45 C.F.R. § 164.402.
 - C. “*Business Associate*” shall have the same meaning as the term “business associate” at 45 C.F.R. § 160.103.
 - D. “*Covered Entity*” shall have the same meaning as the term “covered entity” at 45 C.F.R. § 160.103.
 - E. “*Protected Health Information*” or “*PHI*” shall mean Protected Health Information, as defined in 45 C.F.R. § 160.103, and is limited to the Protected Health Information received, maintained, created or transmitted on behalf of CE by BA in performance of the Services.

For purposes of this Agreement, all references to PHI mean CE's PHI and PHI of Covered Entities for which CE is serving as a Business Associate. PHI shall include Electronic Protected Health Information.

F. "*Unsecured PHI*" shall mean Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS from time to time.

II. **Status of Parties.**

A. BA hereby acknowledges and agrees that CE is a Covered Entity and that BA is a Business Associate of CE.

B. BA acknowledges that BA is directly subject to and shall comply with the HIPAA security standards set forth at 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314 and 164.316 and with any and all applicable HIPAA privacy-related requirements.

C. To the extent BA carries out CE's obligations under HIPAA, BA will comply with the requirements that apply to CE in the performance of such obligations.

III. **Permitted Uses and Disclosures.**

A. *Performance of Services.* BA may use or disclose PHI in connection with the performance of the Services if such use or disclosure of PHI would not violate HIPAA if done by CE or if such use or disclosure is expressly permitted under this Agreement. In performing the Services, BA may request, use, disclose or transmit only the minimum necessary PHI, in accordance with HIPAA.

B. *Proper Management and Administration.* BA may use or disclose PHI received by BA in its capacity as BA of CE for the proper management and administration of BA. Any such disclosure of PHI shall only be made if BA obtains reasonable assurances from the person to whom the PHI is disclosed that: (1) the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; (2) BA will be notified by such person of any instances of which it becomes aware in which the confidentiality of the PHI has been breached; and (3) the person will provide CE, in accordance with Section III C. hereof, appropriate notice and opportunity to object before disclosing PHI on the basis that such disclosure is required by law.

C. *Disclosures Required By Law.* BA may only use or disclose PHI on the basis that such disclosure is required by law after notifying CE's Privacy Officer or his/her designee to allow an opportunity to object to the disclosure and to seek appropriate relief. If CE objects to such disclosure, BA shall, to the extent legally permitted, refrain from disclosing the PHI until CE has exhausted all alternatives for relief. However, if BA is unable to notify CE for reasons beyond BA's control, BA may disclose PHI on the basis that such disclosure is required by law so long as BA provides immediate notice to CE's Privacy Officer or his/her designee following the disclosure.

D. *Disclosure to Subcontractors.* BA shall ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of BA agree, in a writing that complies with the requirements of 45 C.F.R. § 164.504(e)(2) through (e)(4), to be bound by the same

restrictions and conditions that apply to BA under this Agreement with respect to such PHI, including, without limitation, implementing reasonable and appropriate safeguards to protect it.

E. *Data Aggregation.* To the extent permitted by the Underlying Agreement, or as otherwise expressly agreed to in writing by CE, BA may use and disclose PHI for data aggregation purposes, however, only in order to analyze data for permitted health care operations of CE, and only to the extent that such use is permitted under HIPAA.

F. *De-identified Information.* BA may not de-identify PHI without CE's prior written consent. BA may only use and disclose de-identified health information if (i) the use is disclosed to CE and permitted by CE in writing in its sole discretion and (ii) the de-identification is in compliance with 45 C.F.R. § 164.502(d), and the de-identified health information meets the standards and implementation specifications for de-identification under 45 C.F.R. § 164.514(a) and (b).

IV. **Nondisclosure.**

A. *As Provided In Agreement.* BA shall not use or further disclose PHI except as permitted or required by this Agreement.

B. *Additional Restrictions.* If CE notifies BA that CE has agreed to be bound by additional restrictions on the uses or disclosures of PHI pursuant to HIPAA, BA and CE shall mutually agree on the extent to which BA will be bound by such additional restrictions and BA shall not disclose PHI in violation of such additional mutually agreed upon restrictions. BA shall ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of BA agree in writing to be bound to such restrictions mutually agreed upon between BA and CE.

V. **Safeguards, Reporting, Mitigation and Enforcement.**

A. *Safeguards.* BA shall use any and all appropriate safeguards to prevent use or disclosure of PHI other than as provided by this Agreement. BA shall, in accordance with HIPAA, timely implement, and require its agents and subcontractors to timely implement, administrative, physical and technical safeguards, and policies and procedures, that reasonably and appropriately protect the confidentiality, integrity, and availability of any PHI it creates, receives, maintains or transmits on behalf of the CE.

B. *Reporting.* BA shall report to CE's Privacy Officer or his/her designee as soon as practicable, but in no event more than ten (10) days, after BA becomes aware of (1) any use or disclosure of PHI in violation of this Agreement or applicable law or (2) any Security Incident as defined by HIPAA at 45 C.F.R. §164.304.

C. *Mitigation.* BA shall have procedures in place to mitigate, to the maximum extent practicable, any deleterious effect from any use or disclosure of PHI in violation of this Agreement or applicable law.

D. *Sanctions.* BA shall maintain appropriate sanction policies and apply them against any employee, subcontractor or agent who uses or discloses PHI in violation of this Agreement or applicable law.

E. *United States Department of Health and Human Services.* BA shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary of the United States Department of Health and Human Services (“HHS”) for purposes of determining CE’s compliance with HIPAA; provided, however, that BA shall immediately notify CE upon receipt by BA of any such request for access by the Secretary of HHS, and shall provide CE with a copy thereof as well as a copy of all materials disclosed pursuant thereto. The parties’ respective rights and obligations under this Section V E. shall survive termination of the Agreement.

VI. **Obligation to Provide Access, Amendment and Accounting of PHI.**

A. *Access to PHI.* BA shall make available to CE such information as CE may require to fulfill CE’s obligations to provide access to, and copies of, PHI in accordance with HIPAA.

B. *Amendment of PHI.* BA shall make available to CE such information as CE may require to fulfill CE’s obligations to amend PHI in accordance with HIPAA. In addition, BA shall, as directed by CE, incorporate any amendments to PHI into copies of such information maintained by BA.

C. *Accounting of Disclosures of PHI.* BA shall make available to CE such information as CE may require to fulfill CE’s obligations to provide an accounting of disclosures with respect to PHI in accordance with HIPAA. In addition, BA shall maintain a record of all disclosures of PHI, including the date of the disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure which includes an explanation of the basis for such disclosure. BA shall make this record available to CE upon CE’s request.

D. *Restrictions on Disclosures to Health Plans.* BA agrees to take all necessary steps, at the request of CE, to comply with requests by individuals not to send PHI to health plans in accordance with 45 C.F.R. § 164.522(a). BA may not agree to any restriction on the use or disclosure of PHI requested by an individual without CE’s prior approval.

E. *Forwarding Requests From Individual.* In the event that any individual requests access to, amendment of, accounting of, or restrictions on the use or disclosure of, PHI directly from BA, BA shall within three (3) business days forward such request to CE. CE shall have the responsibility of responding to forwarded requests. However, if forwarding the individual’s request to CE would cause CE or BA to violate HIPAA, BA shall instead respond to the individual’s request as required by such law and notify CE of such response as soon as practicable.

VII. **Reporting of Breaches and Improper Disclosures.**

A. *Notification of Breach, Mitigation.* In the event of a Breach of any Unsecured PHI that BA accesses, maintains, retains, modifies, records, stores, transmits, destroys, or otherwise holds or uses on behalf of CE, BA shall report such Breach to CE as soon as practicable, but in no event more than ten (10) days after the Breach is discovered by BA (as defined in 45 C.F.R. § 164.410(a)). BA shall, in consultation with CE, mitigate, to the extent practicable, any harmful effect of such Breach that is known to BA.

B. *Content of Notification.* Notice of a Breach shall include, at a minimum: (i) the identification of each individual whose Protected Health Information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed during the Breach, (ii) the date of the Breach and the date of discovery of the Breach, if known, (iii) the scope of the Breach, (iv) a description of the BA's response to the Breach, and (v) any other information that CE is required to include in notifications to such individuals pursuant to 45 C.F.R. § 164.404. However, BA's inability to determine such information shall not be cause for delaying notification to the CE.

C. *Notice to Individuals and Media.* CE shall decide how and when the notification to individuals and media shall be provided and shall approve the content of such notifications. If a Breach is attributable to a breach of this Agreement by BA or a violation of HIPAA by BA, at the request of CE and in CE's sole discretion, BA shall provide the notification to individuals and/or the media as directed by CE, and/or reimburse CE, pursuant to Section VII D., for the cost of notifying individuals and/or the media.

D. *Reimbursement of Costs.* To the extent any Breach of Unsecured PHI or security breach under applicable State privacy or information security laws is attributable to either: (i) a breach of the obligations under this Agreement by BA or (ii) a violation of HIPAA or a State's privacy or information security laws by BA, BA shall bear (a) the costs incurred by CE in complying with its legal obligations relating to such breach or violation, and (b) in addition to other damages for which BA may be liable under this Agreement, the following expenses incurred by CE in responding to such breach: (1) the cost of preparing and distributing notifications to affected individuals, (2) the cost of providing notice to government agencies, credit bureaus, the media, and/or other required entities, (3) the cost of providing affected individuals with credit monitoring services to the extent the breach could lead to a compromise of the data subject's credit or credit standing, (4) call center support for such affected individuals and (5) the cost of any other measures required under applicable law.

E. *Indemnification.* Each party (the "Indemnifying Party") agrees to indemnify, defend and hold harmless the other party (the "Indemnified Party"), its directors, officers, employees and agents from any and all liabilities, claims, damages, loss and costs (including reasonable attorneys' fees) to the extent they arise from the negligent acts or omissions or willful misconduct of the Indemnifying Party, or of the Indemnifying Party's directors, officers, employees, or agents, related to this Agreement and/or a violation of HIPAA related to this Agreement.

F. *Tracking of Disclosures.* BA shall track all disclosures of PHI to third parties, including those made to BA's directors, officers, subcontractors, employees, affiliates, agents, and representatives, other than those disclosures that meet the exception criteria of 45 C.F.R. § 164.528.

VIII. Material Breach, Enforcement and Termination.

A. *Term.* This Agreement shall be effective as of the Agreement Effective Date, and shall continue until the Agreement is terminated in accordance with the provisions of Section VIII B. or until the Underlying Agreement terminates, whichever is sooner.

B. *Termination.* CE may terminate this Agreement and the Underlying Agreement:

1. Immediately if CE determines that BA has breached or violated a material term of this Agreement that is not cured within fifteen (15) days of BA's receipt of notice of the breach or violation from CE;
2. Immediately if BA is named as a defendant in a criminal proceeding for a violation of HIPAA;
3. Immediately if a finding or stipulation that BA has violated any standard or requirement of HIPAA or other security or privacy laws is made in any administrative, civil, or criminal proceeding in which BA has been joined; or
4. Pursuant to Section IX B. of this Agreement.
5. If there is no Underlying Agreement, this Agreement may be terminated upon 30 days' written notice from CE to BA.

C. *Knowledge of Non-Compliance.* Any non-compliance by BA with this Agreement or with HIPAA automatically will be considered a breach or violation of a material term of this Agreement if BA knew or reasonably should have known of such non-compliance and failed to immediately take reasonable steps to cure the non-compliance.

D. *Reporting to United States Department of Health and Human Services.* If CE's efforts to cure any breach or end any violation are unsuccessful, and if termination of this Agreement is not feasible, CE may report BA's breach or violation to the Secretary of HHS, and BA agrees that it shall not have or make any claim(s), whether at law, in equity, or under this Agreement, against CE with respect to such report(s).

E. *Return or Destruction of Records.* Upon termination of this Agreement for any reason, BA shall return or destroy, as specified by CE, all PHI that BA still maintains in any form, and shall retain no copies of such PHI. If CE, in its sole discretion, requires that BA destroy any or all PHI, BA shall certify to CE that the PHI has been destroyed. If return or destruction is not feasible, BA shall inform CE of the reason it is not feasible and shall continue to extend the protections of this Agreement to such PHI and limit further use and disclosure of such PHI to those purposes that make the return or destruction of such PHI infeasible.

F. *Injunctions.* CE and BA agree that any violation of the provisions of this Agreement may cause irreparable harm to CE. Accordingly, in addition to any other remedies available to CE at law, in equity, or under this Agreement, in the event of any violation by BA of any of the provisions of this Agreement, or any explicit threat thereof, CE shall be entitled to an injunction or other decree of specific performance with respect to such violation or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages. The parties' respective rights and obligations under this Section VIII F. shall survive termination of the Agreement.

IX. **Miscellaneous Terms.**

A. *State Law.* Nothing in this Agreement shall be construed to require BA to use or disclose PHI without a written authorization from an individual who is a subject of the PHI, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure.

B. *Amendment.* CE and BA agree that amendment of this Agreement may be required to ensure that CE and BA comply with changes in state and federal laws and regulations relating to the privacy, security, and confidentiality of PHI. CE may terminate this Agreement and the Underlying Agreement upon thirty (30) days written notice in the event that BA does not promptly enter into an amendment that CE, in its sole discretion, deems sufficient to ensure that CE will be able to comply with such laws and regulations.

C. *No Third Party Beneficiaries.* Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than CE and BA, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

D. *Ambiguities/Primacy.* The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable law protecting the privacy, security and confidentiality of PHI, including, but not limited to, HIPAA. To the extent that any provisions of this Agreement conflict with the provisions of any other agreement or understanding between the parties, including the Underlying Agreement, this Agreement shall control with respect to the subject matter of this Agreement.

E. *Prohibition of Offshore Disclosure.* BA shall not access, store, share, maintain, transmit, use or disclose PHI in any form via any medium with any entity or person, including BA's employees and subcontractors, beyond the boundaries and jurisdiction of the United States without express written authorization from CE, which may be withheld, delayed or conditioned in CE's discretion.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Agreement Effective Date.

MAIMONIDES MEDICAL CENTER By:  Joyce A. Leahy, Esq. Privacy Officer/EVP for Legal Affairs & General Counsel	By: _____ Name: Title:
--	------------------------------

BA Contact Information (to be completed by BA)

Primary Contact (Name) : _____
Primary Contact (Telephone): _____
Primary Contact (Email): _____
Security Officer (Name): _____
Security Officer (Telephone): _____
Security Officer (Email): _____