

Musick Dermatology and Advanced Clinical Spa, LLC
4948 Benchmark Centre Drive
Swansea, IL 62226
Phone: (618) 628-2588 Fax: (618) 628-1363
www.MusickDermatology.com

HIPAA Business Associate Agreement

This HIPAA Business Associate Agreement is executed by the parties on the dates shown beneath their respective signature lines, but is effective as of January 1, 2019 by and between Musick Dermatology and Advanced Clinical Spa, LLC and (*stated business associate*).

WHEREAS, (*stated business associate*) may maintain, transmit create or receive data for or from Musick Dermatology and Advanced Clinical Spa, LLC that constitutes Protected Health Information (as defined at 45 CFR §160.103) to perform tasks on behalf of Musick Dermatology and Advanced Clinical Spa, LLC.

WHEREAS, Musick Dermatology and Advanced Clinical Spa, LLC is or may be subject to the requirements of 42 U.S.C. 1320d et seq. enacted by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act (“HITECH”) and the implementing regulations set forth at 45 CFR Parts 160, 162 and 164 (“HIPAA Regulations”). As used herein, “PHI” refers to Protected Health Information maintained, transmitted, created or received by (*stated business associate*) for or from Musick Dermatology and Advanced Clinical Spa.

WHEREAS, to the extent required by the HIPAA Regulations and applicable state law, (*stated business associate*) is or may be directly subject to certain privacy and security obligations and penalty provisions of HIPAA, HITECH, the HIPAA Regulations and state law.

NOW, THEREFORE, the parties agree as follows:

1. (*Stated business associate*) may use and disclose PHI only as expressly permitted or required by this Agreement or as required by law. (*Stated business associate*) may use or disclose PHI as required to perform [***use the following if a written service agreement exists***: its obligations under any underlying service agreements (collectively, “Service Agreement”) between the parties to perform certain services as described in the Service Agreement (“Services”)] [***use the following if there is NOT a written service agreement in place***: the following services on behalf of Musick Dermatology and Advanced Clinical Spa, LLC: _____ . (the “Services”)] , provided that (*stated business*

associate) shall not use or disclose PHI in any manner that would constitute a violation of the HIPAA Regulations if done by Musick Dermatology and Advanced Clinical Spa, LLC. Without limiting the generality of the foregoing, *(stated business associate)* shall not sell PHI or use or disclose PHI for purposes of marketing or fundraising, as defined and proscribed in the HIPAA Regulations, HITECH and applicable state law. *(Stated business associate)* shall limit its uses and disclosures of, and requests for, PHI (i) when practical, to the information making up a limited data set (as set forth at 45 CFR § 164.514); and (ii) in all other cases subject to the requirements of 45 CFR §164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request. To the extent Musick Dermatology and Advanced Clinical Spa, LLC notifies *(stated business associate)* of a restriction request granted by Musick Dermatology and Advanced Clinical Spa, LLC that would limit *(stated business associate)*'s use or disclosure of PHI, *(stated business associate)* will comply with the restriction. To the extent *(stated business associate)* is to carry out an obligation of Musick Dermatology and Advanced Clinical Spa, LLC under the HIPAA Regulations, *(stated business associate)* shall comply with the requirements of the HIPAA Regulations that apply to Musick Dermatology and Advanced Clinical Spa, LLC in the performance of such obligation.

2. *(Stated business associate)* agrees to use and maintain reasonable and appropriate administrative, technical and physical safeguards to protect PHI from uses or disclosures not permitted by this Agreement, including, but not limited to, maintaining policies and procedures to detect, prevent or mitigate identity theft based on PHI or information derived from PHI. In addition, *(stated business associate)* agrees to comply with the applicable requirements of 45 CFR Part 164, subpart C of the HIPAA Regulations with respect to electronic PHI and any guidance issued by the Secretary of the Department of Health and Human Services ("HHS"). *(Stated business associate)* specifically agrees to employ multiple security mechanisms to ensure the confidentiality, integrity and availability of all electronic PHI, including, but not limited to, authentication controls, authorization controls, audit controls and encryption.
3. To the extent *(stated business associate)* becomes aware of or discovers any use or disclosure of PHI in violation of this Agreement, any Security Incident (as defined at 45 CFR §164.304) any Red Flag (as defined at 16 CFR §681.2(b)) related to any individual who is the subject of PHI, and any Breach of Unsecured Protected Health Information (both as defined at 45 CFR §164.402), *(stated business associate)* shall promptly report such use, disclosure, incident, Red Flag or breach to Musick Dermatology and Advanced Clinical Spa, LLC. All reports of Breaches shall be made within ten (10) business days of *(stated business associate)* discovering the Breach and shall include the information specified at 45 CFR § 164.410. *(Stated business associate)* shall mitigate, to the extent practicable, any harmful effect known

- to it of a use or disclosure of PHI by (*stated business associate*) not permitted by this Agreement. (*Stated business associate*) shall promptly reimburse Musick Dermatology and Advanced Clinical Spa, LLC all reasonable costs incurred by Musick Dermatology and Advanced Clinical Spa, LLC with respect to providing notification of and mitigating a Breach involving (*stated business associate*), including but not limited to printing, postage costs and toll-free hotline costs.
4. In accordance with 45 CFR §§ 164.308(b)(2) and 164.502(e)(1)(i), (*stated business associate*) shall ensure that each subcontractor or agent that creates, receives, maintains, or transmits PHI on behalf of (*stated business associate*) agrees in writing to be bound by the same restrictions, terms and conditions that apply to (*stated business associate*) pursuant to this Agreement.
 5. In accordance with 45 CFR §164.524 and within fifteen (15) days of a request by Musick Dermatology and Advanced Clinical Spa, LLC for access to PHI about an individual contained in a Designated Record Set (as defined at 45 CFR §164.501), (*stated business associate*) shall make available to Musick Dermatology and Advanced Clinical Spa, LLC such PHI in the form requested by Musick Dermatology and Advanced Clinical Spa, LLC. If the requested PHI is maintained electronically, (*stated business associate*) shall provide a copy of the PHI in the electronic form and format requested by the individual, if it is readily producible, or, if not, in a readable electronic form and format as agreed to by Musick Dermatology and Advanced Clinical Spa, LLC and the individual. In the event that any individual requests access to PHI directly from (*stated business associate*), (*stated business associate*) shall within ten (10) days forward such request to Musick Dermatology and Advanced Clinical Spa, LLC. Any denials of access to the PHI requested shall be the responsibility of Musick Dermatology and Advanced Clinical Spa, LLC.
 6. In accordance with 45 CFR §164.526 and within fifteen (15) days of receipt of a request from Musick Dermatology and Advanced Clinical Spa, LLC for the amendment of an individual's PHI contained in a Designated Record Set (for so long as the PHI is maintained in the Designated Record Set), (*stated business associate*) shall provide such information to Musick Dermatology and Advanced Clinical Spa, LLC for amendment and incorporate any such amendments in the PHI as required by 45 CFR §164.526. In the event a request for an amendment is delivered directly to (*stated business associate*), (*stated business associate*) shall within ten (10) days of receiving such request forward the request to Musick Dermatology and Advanced Clinical Spa, LLC.
 7. Except for disclosures of PHI by(*stated business associate*) that are excluded from the accounting obligation as set forth at 45 CFR §164.528 or regulations issued pursuant to HITECH, (*stated business associate*) shall record for each disclosure the information required to be recorded by covered entities pursuant to 45 CFR §164.528.

Within twenty (20) days of notice by Musick Dermatology and Advanced Clinical Spa, LLC to *(stated business associate)* that it has received a request for an accounting of disclosures of PHI, *(stated business associate)* shall make available to Musick Dermatology and Advanced Clinical Spa, LLC, or if requested by Musick Dermatology and Advanced Clinical Spa, LLC, to the individual, the information required to be maintained pursuant to this Section 7. In the event the request for an accounting is delivered directly to *(stated business associate)*, *(stated business associate)* shall within ten (10) days forward such request to Musick Dermatology and Advanced Clinical Spa, LLC.

8. At Musick Dermatology and Advanced Clinical Spa, LLC's or HHS' request, *(stated business associate)* shall make its internal practices, books and records relating to the use and disclosure of PHI available to HHS for purposes of determining compliance with the HIPAA Regulations.
9. *(Stated business associate)* is not authorized to use or disclose PHI in a manner that would violate the HIPAA Regulations if done by Musick Dermatology and Advanced Clinical Spa, LLC, provided that *(stated business associate)* may:
 - a. Use the PHI for its proper management and administration and to carry out its legal responsibilities.
 - b. Disclose PHI for its proper management and administration and to carry out its legal responsibilities, provided that disclosures are required by law, or *(stated business associate)* obtains reasonable assurances from the recipient that the PHI will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the recipient, and the recipient notifies *(stated business associate)* of any instances of which it is aware in which the confidentiality of the information has been breached.
 - c. Use and disclose PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).
 - d. Aggregate the PHI in its possession with the Protected Health Information of other covered entities that *(stated business associate)* has in its possession through its capacity as a business associate to other covered entities, provided that the purpose of such aggregation is to provide Musick Dermatology and Advanced Clinical Spa, LLC with data analysis relating to the health care operations of Musick Dermatology and Advanced Clinical Spa, LLC.
 - e. Use PHI to create de-identified information, provided that the de-identification conforms to the requirements of 45 CFR § 164.514(b).
10. If *(stated business associate)* conducts standard transactions (as defined in 45 CFR Part 160) for or on behalf of Musick Dermatology and Advanced Clinical Spa, LLC *(stated business associate)* will comply and will require by written contract each agent or contractor (including any subcontractor) involved with the conduct of such standard transactions to comply, with each applicable requirement of the HIPAA Regulations (as set forth at 45 CFR Parts 160 and 162). *(Stated business associate)*

will not enter into, or permit its agents or contractors (including subcontractors) to enter into, any trading partner agreement in connection with the conduct of standard transactions for or on behalf of Musick Dermatology and Advanced Clinical Spa, LLC that: (i) changes the definition, data condition, or use of a data element or segment in a standard transaction; (ii) adds any data elements or segments to the maximum defined data set; (iii) uses any code or data element that is marked “not used” in the standard transaction’s implementation specification or is not in the standard transaction’s implementation specification; or (iv) changes the meaning or intent of the standard transaction’s implementation specification. (*Stated business associate*) agrees to participate in any test modification conducted by Musick Dermatology and Advanced Clinical Spa, LLC in accordance with the HIPAA Regulations.

11. A. [use the following if a written service agreement exists: This Agreement shall be effective as the Effective Date and shall remain in effect until the Service Agreement is terminated or expires. Either party may terminate this Agreement and the Service Agreement effective immediately if it determines that the other party has breached a material provision of this Agreement and failed to cure such breach within thirty (30) days of being notified by the other party of the breach. If the non-breaching party determines that cure is not possible, such party may terminate this Agreement and the Service Agreement effective immediately upon written notice to other party. If termination is not feasible, the non-breaching party shall report the breach to HHS. The parties understand and agree that termination of this Agreement shall constitute a default by (*stated business associate*) under the Service Agreement.

B. [use the following instead if there is NOT a written service agreement in place: This Agreement shall be effective as of the Effective Date and shall remain in effect until (*stated business associate*) ceases to provide the Services to Musick Dermatology and Advanced Clinical Spa, LLC.. Either party may terminate this Agreement effective immediately if it determines that the other party has breached a material provision of this Agreement and failed to cure such breach within thirty (30) days of being notified by the other party of the breach. If the non-breaching party determines that cure is not possible, such party may terminate this Agreement effective immediately upon written notice to other party. If termination is not feasible, the non-breaching party shall report the breach to HHS. The parties understand and agree that termination of this Agreement shall automatically terminate the relationship whereby (*stated business associate*) performs the Services on behalf of the Musick Dermatology and Advanced Clinical Spa, LLC.]

12. Upon termination of this Agreement, (*stated business associate*) shall either return or destroy, at no cost to Musick Dermatology and Advanced Clinical Spa, LLC all PHI that (*stated business associate*) still maintains in any form. (*Stated business associate*) shall not retain any copies of such PHI. Notwithstanding the foregoing, to the extent that it is not feasible to return or destroy such PHI, the terms and provisions of this Agreement shall survive termination of this Agreement, and (*stated business*

associate) shall only use or disclose such PHI solely for such purpose or purposes which prevented the return or destruction of such PHI.

13. Nothing in this Agreement shall be construed to create any rights or remedies in any third parties or any agency relationship between the parties. To the extent (*stated business associate*) is acting as a business associate under the HIPAA Regulations, (*stated business associate*) shall be subject to the penalty provisions specified in HITECH. Upon the effective date of any final regulation or amendment to final regulations promulgated by HHS with respect to PHI, this Agreement will be deemed to be automatically amended such that the obligations imposed on the parties remain in compliance with such regulations. The terms and conditions of this Agreement shall override and control any conflicting term or condition of any agreement between the parties with respect to the Services [include the following if a written service agreement exists: including the Service Agreement], and all non-conflicting terms and conditions shall remain in full force and effect.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement on the dates set forth below.

Musick Dermatology and
Advanced Clinical Spa, LLC

(*stated business associate*)

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____