**BUSINESS ASSOCIATE AGREEMENT**

Please complete the following and return signed

via Fax:

618-288-7866

via Mail:

MidAmerica Plastic Surgery
Attn: Privacy Officer
6812 State Route 162
Suite 21
Maryville, IL 62062

## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into by and between _____ ("Business Associate") and Ryan S. Diederich, MD, PC. d/b/a MidAmerica Plastic Surgery, on its own behalf and on behalf of all present and future entities that are part of its Affiliated Covered Entity (individually and collectively, "Provider") effective as of _____ ("Effective Date").

## RECITALS

A. Under the privacy regulations ("Privacy Regulations") and security regulations ("Security Regulations") promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended, and the Health Information Technology for Economic and Clinical Health Act of 2009 and the regulations promulgated thereunder, as amended, (collectively, "HITECH Act"), Provider is required to enter into agreements with Provider's business associates to assure that Provider's business associates appropriately safeguard protected health information.

B. Business Associate provides _____ ("Services") for or on behalf of Provider pursuant to the terms of the agreement between the parties ("Service Agreement"), and in connection with providing the Services, Business Associate may access, create, maintain or transmit certain Protected Health Information ("Provider PHI").

C. The parties desire to enter into this Agreement to protect the privacy and security of Provider PHI in compliance with the Privacy Regulations, the Security Regulations and the HITECH Act.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. **Definitions.** All terms used in this Agreement and defined in the Privacy Regulations, Security Regulations or HITECH Act shall have the meaning ascribed to them in the Privacy Regulations, Security Regulations or HITECH Act, as applicable.

2. **Rights of Business Associate.** Business Associate is permitted to use and disclose Provider PHI as necessary to perform Services for or on behalf of Provider, subject to the terms of this Agreement.

3. **Obligations of Business Associate.** With regard to the use and disclosure of Provider PHI, Business Associate agrees as follows:

   (a) **Use and Disclosure of Provider PHI.** In providing Services, Business Associate shall use and disclose Provider PHI only as permitted by the terms of this Agreement or required by law and only to the extent that such use and disclosure would not violate the Privacy Regulations, Security Regulations or HITECH Act if performed by Provider. Notwithstanding the foregoing, Business Associate may use and disclose Provider PHI received in its capacity as a Business Associate if necessary for the proper management and administration of the Business Associate, provided that Business Associate may disclose Provider PHI to third parties not employed by Business Associate only if (i) the disclosure is required by law, or (ii) Business Associate obtains reasonable assurances from the recipient that (A) the Provider PHI 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 recipient, and (B) the recipient will notify Business Associate of any breach of confidentiality of Provider PHI. Upon prior written request of Provider, Business Associate may use Provider PHI to provide data aggregation services related to the healthcare operations of the Provider. Notwithstanding anything herein to the contrary, Business Associate may not de-identify Provider PHI unless Business Associate obtains the prior written consent of Provider and then such de-identification must be consistent with the de-identification requirements of the Privacy Regulations and any use or disclosure of the de-identified information may only be for purposes approved in writing by Provider.

(b) **Safeguards.** Business Associate shall implement and at all times use all appropriate safeguards and shall comply with the Security Regulations with respect to electronic PHI to prevent any use or disclosure of Provider PHI not authorized under this Agreement.

(c) **Reporting.** Business Associate shall report in writing to Privacy Officer of Provider, no later than one (1) day after the incident, any use or disclosure of Provider PHI not permitted under the terms of this Agreement of which Business Associate becomes aware, including, without limitation, any Breach of Unsecured Protected Health Information and any Security Incident, it being agreed that unsuccessful attempts of unauthorized access, use, disclosure, modification or destruction of electronic PHI or unsuccessful attempts at interference with systems operations in an information system containing electronic PHI shall be reported by Business Associate to Provider only upon Provider's request for such information. With respect to any improper uses and disclosures of Provider PHI that constitute or may constitute a Breach of Unsecured PHI, or a data breach under applicable state law, Business Associate's report shall include: (i) a brief description of the incident, including the date of the incident, the date of the discovery of the incident and identification of each patient whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, improperly accessed, acquired, used or disclosed, (ii) a description of the types of Unsecured PHI involved in the incident, (iii) any steps the patient should take to protect himself or herself from harm resulting from the incident, (iv) a brief description of what Business Associate is doing to investigate the incident, to mitigate the harm to the patient and to protect against future occurrences; and (v) any other relevant information. Upon providing such report to Provider, Business Associate shall fully cooperate with Provider to enable Provider to conduct a risk assessment and determine whether the incident resulted in a Breach of Unsecured PHI or a data breach under applicable state law. If it is determined by Provider that the incident resulted in a Breach of Unsecured PHI or a data breach under applicable state law, Business Associate shall fully cooperate with Provider and assist Provider in taking all actions required to comply with the HITECH Act and any applicable state law. If Provider requests in writing that Business Associate send notification letters to the affected individuals or any other party regarding such incident as required under the HITECH Act or applicable state law, Business Associate shall (A) promptly send such notification letters at Business Associate's sole expense, (B) comply with the HITECH Act and applicable state law with respect to the timing, content and other requirements pertaining to such letters, and (C) obtain Provider's written approval of such letters prior to sending such letters to the affected individuals or any other party. Business Associate shall not provide any

notification to any party regarding such incident without obtaining prior written consent of Provider. Notwithstanding any provision of the Service Agreement, Business Associate shall promptly reimburse Provider for all documented costs incurred by Provider in connection with such incident, including, without limitation, the cost of providing required notifications, legal fees, fees related to credit monitoring services for the affected individuals, as well as for the amount of any monetary fines or penalties imposed on Provider by the DHHS, any State Attorney General, any other governmental authority or a court of law in connection with such incident. Business Associate shall maintain documentation of such incident as required by the HITECH Act and any applicable state law, including all information that will need to be reported to DHHS or other governmental authorities in connection with such incident. The provisions of this Section shall survive termination of this Agreement for any reason.

(d) **Subcontractors.** Business Associate shall enter into a written agreement with all subcontractors that create, receive, maintain or transmit Provider PHI on behalf of Business Associate which agreement shall require such subcontractors to agree to the same restrictions, conditions and requirements that apply under this Agreement to Business Associate with respect to Provider PHI.

(e) **Mitigation.** Business Associate shall take any and all actions necessary to promptly mitigate any harmful effects known to Business Associate to result from an unauthorized use or disclosure of Provider PHI by Business Associate or its subcontractors.

(f) **Access to PHI.** To enable Provider to respond to a patient's request to access the patient's PHI as required by the Privacy Regulations, Business Associate shall make the patient's PHI maintained by Business Associate in a Designated Record Set available to Provider for inspection and copying within five (5) business days of receiving Provider's request for access. If Business Associate uses or maintains an electronic health record with respect to Provider PHI, Business Associate shall provide such PHI in electronic format, if requested, to enable Provider to fulfill its obligations under the HITECH Act and the Privacy Regulations.

(g) **Amendment of PHI.** To enable Provider to respond to a patient's request to amend the patient's PHI as required by the Privacy Regulations, Business Associate shall make the requested PHI maintained by Business Associate in a Designated Record Set available to Provider within ten (10) business days of receiving a request from Provider and incorporate any necessary amendment into the patient's PHI as directed by Provider.

(h) **Accounting of Disclosures.** To enable Provider to respond to a patient's request for accounting of disclosures of the patient's PHI as required by the Privacy Regulations, Business Associate shall (i) document all disclosures of Provider PHI by Business Associate which Provider would be required to include in its response to an accounting request under the Privacy Regulations and the HITECH Act, and (ii) within five (5) business days of receiving a request for accounting from Provider, make available to Provider the following information concerning such disclosures: the date of disclosure; the name of the recipient and, if known, the recipient's address; a brief description of the PHI disclosed; and a brief statement of the purpose of the disclosure.

(i) **Disclosures to Secretary of DHHS.** Business Associate shall (i) make all internal practices, books and records relating to the use and disclosure of Provider PHI received or created by Business Associate on behalf of Provider available to the Secretary of

DHHS for the purpose of determining Provider's or Business Associate's compliance with the Privacy Regulations or the Security Regulations, and (ii) provide Provider with a copy of all documents made available to the Secretary of DHHS within three (3) days of providing such documents to DHHS.

(j) **Minimum Necessary.** In using or disclosing Provider PHI and requesting PHI from Provider or other third parties, Business Associate shall use, disclose or request only the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

(k) **Compliance.** Business Associate shall (i) comply with the requirements of the Security Regulations, (ii) comply with the requirements of the Privacy Regulations and the HITECH Act applicable to Business Associate, (iii) maintain and transmit all Provider PHI in a form which complies with DHHS issued guidance regarding securing PHI, and (iv) comply with applicable state data breach laws and other laws concerning use or disclosure of PHI, provided that any patient and other notifications required under such laws shall be made only consistent with the requirements specified in this Agreement. To the extent Business Associate is to carry out a Provider's obligation under the Privacy Regulations, Business Associate shall comply with the requirements of the Privacy Regulations that apply to Provider in the performance of such obligation.

(l) **Compliance With Electronic Transactions and Code Sets Standards.** If Business Associate conducts electronically any of the administrative or financial healthcare transactions identified as "standard transactions" under HIPAA for or on behalf of Provider, Business Associate shall comply with all applicable requirements of the Electronic Transactions and Code Sets Standards promulgated under HIPAA when conducting such standard transactions for or on behalf of Provider.

(m) **Record Retention.** Business Associate shall retain all HIPAA and HITECH Act related documentation pertaining to Provider PHI for at least six (6) years, as required by the Privacy Regulations and other applicable laws. The provisions of this Section shall survive termination of this Agreement for any reason.

4. **Obligations of Provider.** With respect to the use and disclosure of Provider PHI by Business Associate, Provider shall:

(a) Notify Business Associate of any limitation(s) in its notice of privacy practices, to the extent that such limitation(s) would impact Business Associate's use or disclosure of Provider PHI,

(b) Inform Business Associate of any changes in, or revocation of, a patient's authorization to use or disclose the patient's PHI if such action would impact Business Associate's use or disclosure of Provider PHI;

(c) Notify Business Associate of any restrictions on the use and/or disclosure of Provider PHI to which Provider has agreed if such restriction would impact Business Associate's use or disclosure of Provider PHI; and

(d) Not request Business Associate to use or disclose Provider PHI in any manner that would not be permissible under the Privacy Regulations if done by Provider, subject to the provisions of Section 3(a) of this Agreement.

5. **Term and Termination.**

(a) **Term.** Unless earlier terminated pursuant to this Agreement, this Agreement shall be effective on the Effective Date and shall continue in effect until Business Associate no longer provides any services to Provider involving access, creation, maintenance or transmission of Provider PHI.

(b) **Termination by Provider.** Notwithstanding any contrary provisions regarding termination of the Service Agreement contained in the Service Agreement, if Provider determines that Business Associate breached any provision of this Agreement, Provider shall have the right, without incurring liability for damages or penalties as a result of termination of the Service Agreement, to either (i) immediately terminate this Agreement and the Service Agreement, without providing Business Associate an opportunity to cure the breach, upon providing written notice of termination of this Agreement and the Service Agreement to Business Associate, or (ii) provide Business Associate with a written notice of breach and terminate this Agreement and the Service Agreement if Business Associate does not cure the breach to the satisfaction of Provider within thirty (30) calendar days of receiving such notice.

(c) **Termination by Business Associate.** If Business Associate determines, after consultation with Provider, that Provider breached any obligation of Provider under Section 4 of this Agreement, Business Associate shall provide to Provider a written notice of the breach which notice shall include a detailed explanation of the breach. If Provider does not cure such breach within thirty (30) calendar days of receiving such notice, Business Associate shall have the right to terminate this Agreement and the Service Agreement upon providing written notice of termination of this Agreement and the Service Agreement to Provider.

(d) **Effect of Termination.** Upon termination of this Agreement, Business Associate shall immediately return to Provider or destroy, if requested by Provider, Provider PHI possessed by Business Associate or its subcontractors and retain no copies or back-up records of Provider PHI in any form or medium. If such return or destruction is infeasible, Business Associate shall promptly notify Provider in writing of such information and the reasons making the return or destruction of Provider PHI infeasible. To the extent, upon termination of this Agreement, Business Associate does not return to Provider or destroy Provider PHI as required herein, all of Business Associate's obligations set forth in this Agreement related to Provider PHI shall survive termination of the Agreement and Business Associate shall limit any further use and disclosure of Provider PHI to the purposes that make the return or destruction of Provider PHI infeasible. The provisions of this Section shall survive termination of this Agreement for any reason.

6. **Indemnification.** Notwithstanding any limitation of liability or any other provision of the Service Agreement, Business Associate shall indemnify, defend and hold harmless Provider and its directors, officers, members, employees and agents against any and all losses, liabilities, damages, judgments, suits, penalties, fines, claims and demands of any kind, awards and fees, including, without limitation, attorney fees, arising out of or related to any action by Business Associate under this Agreement, a breach of Unsecured PHI or data breach under state law, a breach of this Agreement by Business Associate or any action by any of Business Associate's subcontractors that create, receive, maintain or transmit Provider PHI. The provisions of this Section shall survive termination of this Agreement for any reason.

7. **Independent Contractors.** Provider and Business Associate shall be independent contractors and nothing in this Agreement is intended nor shall be construed to create an agency, partnership, employer-employee, or joint venture relationship between them.

8. **Entire Agreement.** This Agreement constitutes the entire agreement between the parties hereto relating to the subject matter hereof and supercedes any prior or contemporaneous verbal or written agreements, communications and representations relating to the subject matter hereof. Notwithstanding any provision in the Service Agreement indicating that it is the sole agreement governing the relationship between the parties, including a provision that the Service Agreement shall constitute the entire agreement between the parties thereof, the terms of this Agreement shall be effective and shall govern the relationship between the parties with respect to the subject matter hereof. In the event of any inconsistency between the terms of this Agreement and the terms of the Service Agreement, the terms of this Agreement shall prevail with respect to the subject matter hereof notwithstanding any contrary provision in the Service Agreement.

9. **Amendment/Assignment.** This Agreement may be modified or amended only upon mutual written consent of the parties. Notwithstanding the foregoing or any contrary provisions regarding amendment contained in the Service Agreement, the parties agree that this Agreement shall be automatically amended upon written notice of the amendment by Provider to Business Associate, if Provider determines that such amendment becomes required in order for Provider to comply with the Privacy Regulations, Security Regulations, the HITECH Act or any state law. Business Associate may not assign its rights and obligations under this Agreement without the prior written consent of Provider. Provider may assign its rights and obligations under this Agreement upon providing notice of assignment to Business Associate.

10. **Notices.** Any notices to be given hereunder shall be deemed effectively given when personally delivered, received by electronic means (including facsimile, pdf or e-mail) or overnight courier, or five (5) calendar days after being deposited in the United States mail, with postage prepaid thereon, certified or registered mail, return receipt requested, addressed as follows:

If to Business Associate: _____

_____

_____

If to Provider: Ryan S. Diederich, MD, PC. d/b/a MidAmerica Plastic Surgery
6812 State Route 162
Suite 21
Maryville, IL 62062
Attn: Privacy Officer

11. **No Third Party Beneficiaries.** The terms of this Agreement are not intended and shall not be construed to confer upon any person other than the parties hereto any rights, remedies, obligations or liabilities whatsoever.

12. **Waiver.** A waiver by either party of a breach or failure to perform under this Agreement shall not constitute a waiver of any subsequent breach or failure.

13. **Counterparts/Electronic Signatures.** This Agreement may be executed in counterparts, each of which shall be deemed to be an original and all of which together shall constitute one and the same document. A copy of the Agreement bearing a signature transmitted via facsimile or other electronic means shall be deemed to be an original.

14. **Governing Law.** This Agreement shall be governed by, construed, interpreted and enforced under the laws of the state identified in the Service Agreement as the governing state law, provided that in the event the Service Agreement does not identify such a state, this Agreement shall be governed by, construed, interpreted and enforced under the laws of the state of Illinois.

15. **Service Agreement.** In the event the parties have not entered into a Service Agreement, this Agreement shall be interpreted as though the Agreement does not contain any references to a Service Agreement.

16. **Scope.** This Agreement applies to all present and future agreements and relationships, whether written, oral or implied, between Provider and Business Associate, pursuant to which Provider provides Provider PHI to Business Associate in any form or medium whatsoever. This Agreement shall automatically be incorporated into all subsequent agreements between Provider and Business Associate involving the use or disclosure of Provider PHI, whether or not expressly referenced therein.

IN WITNESS WHEREOF, each party has caused this Business Associate Agreement to be duly executed in its name and on its behalf effective as of the Effective Date.

| | |
|---|---|
| _____<br>Business Associate | Ryan S. Diederich, MD, PC d/b/a<br>MidAmerica Plastic Surgery |
| By: _____ | By: _____ |
| Name: _____ | Name: Ryan S. Diederich |
| Title: _____ | Title: President |