RESOLUTION AGREEMENT

I. Recitals

1. Parties. The Parties to this Resolution Agreement ("Agreement") are:

A. The United States Department of Health and Human Services, Office for Civil Rights ("HHS"), which enforces the Federal Standards for the Privacy of Individually Identifiable Health Information (45 C.F.R. Part 160 and Subparts A and E of Part 164, the "Privacy Rule"); the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Part 160 and Subparts A, and C of 45 C.F.R. Part 164, the "Security Rule"), and the Federal standards for Notification in the Case of Breach of Unsecured Protected Health Information (45 C.F.R. Part 160 and Subparts A and D of 45 C.F.R. Part 164, the "Breach Notification Rule"). HHS has the authority to conduct investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules by covered entities, and covered entities must cooperate with HHS' investigation. 45 C.F.R. §160.306(c) and §160.310(b); and

B. Adult & Pediatric Dermatology, P.C. ("Covered Entity"), a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the Privacy, Security, and Breach Notification Rules. The Covered Entity has office locations in Concord, Westford, Marlborough, and Ayer, Massachusetts, and one office in Wolfeboro, New Hampshire.

HHS and the Covered Entity shall together be referred to herein as the "Parties."

2. Factual Background and Covered Conduct. On October 7, 2011, HHS received notification from the Covered Entity regarding a breach of its unsecured electronic protected health information (ePHI). The Covered Entity reported that an unencrypted thumb drive that contained the ePHI relating to the performance of Mohs surgery of approximately 2,200 individuals was stolen from a vehicle of one its workforce members. The thumb drive was never recovered. The Covered Entity notified its patients of the theft of the thumb drive within 30 days of its theft and provided media notice. On November 9, 2011, HHS notified the Covered Entity of HHS's investigation regarding the Covered Entity's compliance with the Privacy, Security, and Breach Notification Rules.

HHS's investigation indicated that the following conduct occurred ("Covered Conduct"):

(1) The Covered Entity did not conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process until October 1, 2012.

(2) The Covered Entity did not fully comply with the administrative requirements of the Breach Notification Rule to have written policies and procedures and train members of its workforce regarding the Breach Notification requirements until February 7, 2012.

(3) On September 14, 2011, the Covered Entity impermissibly disclosed the ePHI of up to 2,200 individuals by providing an unauthorized individual access to said ePHI for a purpose not permitted by the Privacy Rule when it did not reasonably safeguard an unencrypted thumb drive that was stolen from the unattended vehicle of one its workforce members.

3. No Admission. This Agreement is not an admission of liability by the Covered Entity.

4. No Concession. This Agreement is not a concession by HHS that the Covered Entity is not in violation of the Privacy, Security or Breach Notification Rules and that the Covered Entity is not liable for civil money penalties.

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve HHS Complaint No. 12-133708, and any violations of the Privacy, Security and Breach Notification Rules for the Covered Conduct specified in paragraph I.2.of this Agreement. In consideration of the Parties' interest in avoiding the uncertainty, burden and expense of further investigation and formal proceedings, the Parties agree to resolve this matter according to the Terms and Conditions below.

II. Terms and Conditions

1. Payment. The Covered Entity agrees to pay HHS the amount of $150,000.00 ("Resolution Amount"), the payment of which shall be made on behalf of the Covered Entity by its shareholders. The payment of the Resolution Amount shall be made on the Effective Date of this Agreement as defined in paragraph II.9 by electronic funds transfer pursuant to written instructions to be provided by HHS.

2. Corrective Action Plan. The Covered Entity has entered into and agrees to comply with the Corrective Action Plan (CAP), attached as Appendix A, which is incorporated into this Agreement by reference. If the Covered Entity breaches the CAP, and fails to cure the breach as set forth in the CAP, then the Covered Entity will be in breach of this Agreement, and HHS will not be subject to the terms and conditions in the Release set forth in paragraph II.3. of this Agreement.

3. Release by HHS. In consideration of and conditioned upon the Covered Entity's performance of its obligations under this Agreement, HHS releases the Covered Entity from any actions it has or may have against the Covered Entity under the Privacy, Security, and Breach Notification Rules for the Covered Conduct specified -in paragraph I.2. of this Agreement. HHS does not release the Covered Entity from, nor waive any rights, obligations, or causes of action other than those for the Covered Conduct and referred to in this paragraph. This release does not extend to actions that may be brought under section 1177 of the Social Security Act, 42 U.S.C. § 1320d-6.

4. Agreement by Released Party. The Covered Entity shall not contest its obligation to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under this Agreement. The Covered Entity waives all procedural rights granted under section 1128A of the Social Security Act (42 U.S.C. § 1320a-7a), 45 C.F.R. Part 160, Subpart E; and HHS Claims

Collection provisions, 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

5. Binding on Successors. This Agreement is binding on the Covered Entity and its successors, heirs, transferees, and assigns.

6. Costs. Each Party to this Agreement shall bear its own legal and other costs incurred in connection with this matter, including the preparation and performance of this Agreement.

7. No Additional Releases. This Agreement is intended to be for the benefit of the Parties only, and by this instrument the Parties do not release any claims against any other person or entity.

8. Effect of Agreement. This Agreement constitutes the complete agreement between the Parties. All material representations, understandings, and promises of the Parties are contained in this Agreement. Any modifications to this Agreement must be in writing and signed by both Parties.

9. Execution of Agreement and Effective Date. The Agreement shall become effective (i.e., final and binding) on the date of signing of this Agreement and the CAP by the last signatory ("Effective Date").

10. Tolling of Statute of Limitations. Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a civil money penalty ("CMP") must be imposed within six years from the date of the occurrence of the violation. To ensure that this six-year period does not expire during the term of this Agreement, the Covered Entity agrees that the time between the Effective Date of this Agreement and the date this Agreement may be terminated by reason of the Covered Entity's breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the violations which are the subject of this Agreement. The Covered Entity waives and will not plead any statute of limitations, laches, or similar defenses to any actions for the Covered Conduct specified in paragraph I.2. that is filed by HHS within the time period above, except to the extent that such defenses would have been available had an administrative action been filed on the Effective Date of this Agreement.

11. Disclosure. HHS places no restriction on the publication of the Agreement. This Agreement and information related to this Agreement may be made public by either party. In addition, HHS may be required to disclose this Agreement and related material to any person upon request consistent with the applicable provisions of the Freedom of Information Act, 5 U.S.C. § 552, and its implementing regulations, 45 C.F.R. Part 5.

12. Execution in Counterparts. This Agreement may be executed in counterparts, each of which constitutes an original, and all of which shall constitute one and the same agreement.

13. Authorizations. The individual(s) signing this Agreement on behalf of the Covered Entity represents and warrants that it agreed to be bound by the terms of this Agreement and that he/she is authorized to execute this Agreement. The individual signing this Agreement

on behalf of HHS represents and warrants that he is signing this Agreement in his official capacity and that he is authorized to execute this Agreement.

For Adult & Pediatric Dermatology, P.C.

- // -	December 24, 2013
Glenn Smith	Date
Chief Operating Officer	

For the United States Department of Health and Human Services

- // -	December 24, 2013
Peter K. Chan	Date
Regional Manager, Region I	
Office for Civil Rights	

Appendix A CORRECTIVE

ACTION PLAN BETWEEN

THE

DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

ADULT & PEDIATRIC DERMATOLOGY, P.C.

I. Preamble

Adult & Pediatric Dermatology, P.C. ("the Covered Entity"), hereby enters into this Corrective Action Plan ("CAP") with the United States Department of Health and Human Services, Office for Civil Rights ("HHS" or "OCR"). Contemporaneously with this CAP, the Covered Entity is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Agreement as Appendix A. The Covered Entity enters into this CAP as part of the consideration for the release in paragraph II.3. of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

The Covered Entity has identified the following individual as its authorized representative and contact person regarding the implementation of this CAP and for receipt and submission of notifications and reports:

Glenn Smith
Chief Operating Officer
Adult & Pediatric Dermatology
1620 Sudbury Road
Concord, MA 01742

HHS has identified the following individual as its contact person with whom the Covered Entity is to report information regarding the implementation of this CAP:

Ms. Susan Rhodes, Deputy Regional Manager
Office for Civil Rights, Region I
Department of Health and Human Services
JFK Federal Building, Room 1875
Boston, MA 02203
Susan.Rhodes@hhs.gov
Telephone: 617-565-1347
Facsimile: 617-565-3809

The Covered Entity and HHS agree to promptly notify each other of any changes in the contact persons or the other information provided above.

B. Proof of Submissions. Unless otherwise specified, all notifications and reports required by this CAP may be made by any means, including certified mail, overnight mail, or hand delivery, provided that there is proof that such notification was received. For purposes of this requirement, internal facsimile confirmation sheets do not constitute proof of receipt.

III. Effective Date and Term of CAP

The Effective Date of this CAP shall be calculated in accordance with paragraph II.9 of the Agreement ("Effective Date"). The period for compliance with the obligations assumed by the Covered Entity under this CAP shall begin on the Effective Date of this CAP and end on the date OCR approves the Implementation Report specified at paragraph VI ("Compliance Term"). Except that after the Compliance Term ends, the Covered Entity shall still be obligated to comply with the document retention requirement in section VII.

IV. Time

In computing any period of time prescribed or allowed by this CAP, the day of the act, event, or default from which the designated period of time begins to run shall not be included. The last day of the period so computed shall be included, unless it is a Saturday, a Sunday, or a legal holiday, in which event the period runs until the end of the next day that is not one of the aforementioned days.

V. Corrective Action Obligations

The Covered Entity agrees to the following:

A. Security Management Process

1. Within one year following the Effective Date the Covered Entity shall conduct a comprehensive, organizational-wide risk analysis of the ePHI security risks and vulnerabilities that incorporates all of the Covered Entity's electronic media and systems.

2. The Covered Entity shall develop a risk management plan to address and mitigate any security risks and vulnerabilities following the risk analysis specified in paragraph V.A.1 and, if necessary, revise its present policies and procedures. The risk analysis, risk management plan and any revised policies and procedures shall be forwarded to OCR for review and approval within 60 days of the date the Covered Entity completes the risk management plan. OCR shall approve or, if necessary, require revisions to the Covered Entity's risk analysis, risk management plan and any policies and procedures specified above in paragraphs V.A.1 and V.A.2.

3. Upon receiving OCR's notice of required revisions, if any, the Covered Entity shall have 30 days to incorporate the required revisions and provide the revised risk management plan or policies and procedures to OCR for review and approval. If revisions to the Covered Entity's policies and procedures are required, the Covered Entity shall implement,

distribute, and train all appropriate staff members on the revised policies and procedures within 30 calendar days of OCR's approval, in accordance with its applicable administrative procedures for training.

B. Reportable Events

1. During the Compliance Term, the Covered Entity shall, upon receiving information that a workforce member may have failed to comply with any provision of its Privacy, Security, and Breach Notification policies and procedures, promptly investigate the matter. If the Covered Entity, after review and investigation, determines that a member of its workforce has failed to comply with a provision of its Privacy, Security, and Breach Notification policies and procedures, the Covered Entity shall notify OCR in writing within thirty (30) days. Such violations shall be known as "Reportable Events." The report to OCR shall include the following:

a. A complete description of the event, including relevant facts, the persons involved, and the implicated provision(s) of the Covered Entity's Privacy, Security, and Breach Notification policies and procedures; and

b. A description of actions taken and any further steps the Covered Entity plans to take to address the matter, to mitigate the harm, and to prevent it from recurring, including the application of appropriate sanctions against workforce members who failed to comply with its Privacy, Security, and Breach Notification policies and procedures.

2. If no Reportable Events occur during the Compliance Term, the Covered Entity shall advise OCR of this fact in the Implementation Report.

VI. IMPLEMENTATION REPORT

A. Within 60 days after receiving OCR's approval of the risk analysis, risk management plan and any revised policies and procedures consistent with paragraph V.A.3, the Covered Entity shall submit a written report to OCR for review and approval ("Implementation Report"). The Implementation Report shall include:

1. An explanation of how the Covered Entity implemented its security management process consistent with paragraphs V.A.1, V.A.2, and V.A.3 above, focusing specifically on how The Covered Entity determined whether its policies and procedures should be revised based on the risks and vulnerabilities identified in the risk analysis.

2. If revisions to the Covered Entity's policies and procedures were necessary, an attestation signed by an officer of the Covered Entity attesting that any revised policies and procedures have been fully implemented and distributed to all appropriate members of the workforce consistent with the requirements in paragraph V.A.3;

3. If revisions to the Covered Entity's policies and procedures were necessary, an attestation signed by an officer of the Covered Entity attesting that all appropriate members of the workforce have completed training on any revised policies and procedures consistent with the requirements in paragraph V.A.3;

4. A summary of Reportable Events and the status of any corrective and preventative action(s) relating to all such Reportable Events.

5. An attestation signed by an officer of the Covered Entity stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

VII. Document Retention

The Covered Entity shall maintain for inspection and copying all documents and records relating to compliance with this CAP for 3 years from the Effective Date.

VIII. Breach Provisions

The Covered Entity is expected to fully and timely comply with all provisions contained in this CAP.

A. Timely Written Requests for Extensions. The Covered Entity may, in advance of any due date in this CAP, submit a timely written request for an extension of time to perform any act required by this CAP. A "timely written request" is defined as a request in writing received by HHS at least 5 days prior to the date such an act is required or due to be performed.

B. Notice of Breach and Intent to Impose CMP. The Parties agree that a breach of this CAP by the Covered Entity constitutes a breach of the Agreement. Upon a determination by HHS that The Covered Entity has breached this CAP, HHS may notify the Covered Entity of (1) the Covered Entity's breach; and (2) HHS' intent to impose a civil monetary penalty (CMP), pursuant to 45 C.F.R. Part 160, for the Covered Conduct in paragraph I.2. of the Agreement and for any other conduct that constitutes a violation of the HIPAA Privacy, Security, and Breach Notification Rules ("Notice of Breach and Intent to Impose CMP").

C. The Covered Entity Response. The Covered Entity shall have 30 days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS' satisfaction that:

1. the Covered Entity is in compliance with the obligations of this CAP that HHS cited as the basis for the breach;

2. the alleged breach has been cured; or

3. the alleged breach cannot be cured within the 30-day period, but that: (a) the Covered Entity has begun to take action to cure the breach; (b) the Covered Entity is

pursuing such action with due diligence; and (c) the Covered Entity has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30-day period, the Covered Entity fails to meet the requirements of section VIII.C. to HHS' satisfaction, HHS may proceed with the imposition of the CMP against the Covered Entity pursuant to 45 C.F.R. Part 160 for any violations of the Privacy, Security, and Breach Notification Rules for the Covered Conduct in paragraph I.2. of the Agreement and for any other act or failure to act that constitutes a violation of the HIPAA Privacy, Security and Breach Notification Rules. HHS shall notify the Covered Entity in writing of its determination to proceed with the imposition of a CMP.

For Adult & Pediatric Dermatology, P.C.

_____ _____

Glenn Smith Date
Chief Operating Officer

For the United States Department of Health and Human Services

_____ _____

Peter K. Chan Date
Regional Manager, Region I
Office for Civil Rights