

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 that govern the privacy of individually identifiable health information (45 Code of Federal Regulations (C.F.R.) Part 160 and Subparts A and E of Part 164, the "Privacy Rule"), the Federal standards that govern the security of electronic individually identifiable health information 45 C.F.R. Part 160 and Subparts A and C of 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 compliance reviews and investigations of complaints alleging violations of the Privacy, Security, and Breach Notification Rules ("the HIPAA Rules") by covered entities and business associates, and covered entities and business associates must cooperate with HHS compliance reviews and investigations. *See* 45 C.F.R. §§ 160.306(c), 160.308, and 160.310(b).
 - b. Steven A. Porter, M.D., P.C. ("the Practice") is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. Dr. Porter is a board certified gastroenterologist and the sole practitioner of the Practice.

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

2. Factual Background and Covered Conduct

OCR initiated a compliance review of the Practice following the receipt of the Practice's breach report on November 21, 2013. The Practice's breach report claimed that Elevation43, a business associate of Dr. Porter's electronic health record (EHR) company, was impermissibly using the Practice's patients' electronic protected health information ("ePHI") by blocking the Practice's access to such ePHI until Dr. Porter paid Elevation43 \$50,000. OCR's investigation of the Practice revealed that the Practice demonstrated significant noncompliance with the HIPAA Rules, and the following Covered Conduct occurred:

- A. The Practice failed to implement policies and procedures to prevent, detect, contain, and correct security violations. Specifically, the Practice has failed to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of all its ePHI. Further, the Practice failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. *See* 45 C.F.R. § 164.308(a)(1)(i).
 - B. The Practice permitted Dr. Porter's EHR company to create, receive, maintain, or transmit ePHI on the Practice's behalf at least since 2013 without obtaining satisfactory assurances that the EHR company will appropriately safeguard the ePHI. *See* 45 C.F.R. § 164.308(b).
3. No Admission. This Agreement is not an admission of liability by the Practice.

4. No Concession. This Agreement is not a concession by HHS that the Practice is not in violation of the HIPAA Rules and not liable for civil money penalties ("CMPs").

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction Complaint Number 14-182122 and any potential violations of the HIPAA Rules related to the Covered Conduct specified in paragraph I.2 of this Agreement. In consideration of the Parties' interest in avoiding 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

6. Payment. HHS has agreed to accept, and the Practice has agreed to pay HHS, the amount of \$100,000 ("Resolution Amount"). The Practice agrees to pay the Resolution Amount on the Effective Date of this Agreement as defined in paragraph II.14 pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. The Practice 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 Practice breaches the CAP, and fails to cure the breach as set forth in the CAP, then the Practice will be in breach of this Agreement and HHS will not be subject to the Release set forth in paragraph II.8 of this Agreement.

8. Release by HHS. In consideration and conditioned upon the Practice's performance of its obligations under this Agreement, HHS releases the Practice from any actions it may have against the Practice under the HIPAA Rules arising out of or related to the Covered Conduct identified in paragraph I.2 of this Agreement. HHS does not release the Practice from, nor waive any rights, obligations, or causes of action other than those arising out of or related to 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 United States Code (U.S.C.) § 1320d-6.

9. Agreement by Released Parties. The Practice shall not contest the validity of its obligations to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under this Agreement. The Practice waives all procedural rights granted under Section 1128A of the Social Security Act (42 U.S.C. § 1320a- 7a) and 45 C.F.R. Part 160 Subpart E, and HHS claims collection regulations at 45 C.F.R. Part 30, including, but not limited to, notice, hearing, and appeal with respect to the Resolution Amount.

10. Binding on Successors. This Agreement is binding on the Practice and its successors, heirs, transferees, and assigns.

11. 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.

12. 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.

13. 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 shall be set forth in writing and signed by all Parties.

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

15. Tolling of Statute of Limitations. Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a 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 Practice agrees that the time between the Effective Date of this Agreement and the date the Agreement may be terminated by reason of the Practice's breach plus one year thereafter, will not be included in calculating the six-year statute of limitations applicable to the violations which are the subject of this Agreement. The Practice waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct identified in paragraph 1.2 that is filed by HHS within the time period set forth 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.

16. Disclosure. HHS places no restriction on the publication of the Agreement.

17. 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.

18. Authorizations. The individual(s) signing this Agreement on behalf of the Practice represents and warrants that they are authorized by the Practice to execute this Agreement. The individual(s) signing this Agreement on behalf of HHS represent and warrant that they are signing this Agreement in their official capacities and that they are authorized to execute this Agreement.



For Steven A. Porter, M.D., P.C.

Steven A. Porter, M.D.
President and CEO
Steven A. Porter, M.D., P.C.

2/26/20
Date

For Department of Health and Human Services



Andrea Oliver
Regional Manager, Rocky Mountain Region
Office for Civil Rights

2/26/20
Date

Appendix A
CORRECTIVE ACTION PLAN

BETWEEN THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
STEVEN A. PORTER, M.D., P.C.

I. Preamble

Steven A. Porter, M.D., P.C. (hereinafter known as "the Practice") hereby enters into this Corrective Action Plan ("CAP") with the United States Department of Health and Human Services, Office for Civil Rights ("HHS"). Contemporaneously with this CAP, the Practice is entering into the Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Agreement as Appendix A. The Practice enters into this CAP as part of consideration for the release set forth in paragraph II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons.

The Practice 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:

Larry Myers
1508 E. Skyline Drive, Suite 600
Ogden, Utah 84405
Telephone: (385) 715-1156

HHS has identified the following individual as its authorized representative and contact person with whom the Practice is to report information regarding the implementation of this CAP:

Andrea Oliver, Regional Manager
U.S. Department of Health and Human Services
Office for Civil Rights – Rocky Mountain Region
1961 Stout Street, Room 08.148
Denver, Colorado 80294
Telephone: (303) 844-7915
Facsimile: (303) 844-2025
Email: Andrea.Oliver@hhs.gov

The Practice and HHS agree to promptly notify each other of any changes to the contact persons or 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 for this CAP shall be calculated in accordance with paragraph II.14 of the Agreement ("Effective Date"). The period for compliance ("Compliance Term") with the obligations assumed by the Practice under this CAP shall begin on the Effective Date of this CAP and end two (2) years from the Effective Date, unless HHS has notified the Practice under Section VIII hereof of its determination that the Practice breached this CAP. In the event of such notification by HHS under Section VIII hereof, the Compliance Term shall not end until HHS notifies the Practice that it has determined the breach has been cured. After the Compliance Term ends, the Practice shall still be obligated to submit the final Annual Report as required by Section VI and comply with the document retention requirement in Section VII. Nothing in this CAP is intended to eliminate or modify the Practice's obligation to comply with the documentation retention requirements in 45 Code of Federal Regulations (C.F.R.) §§ 164.316(b) and 164.530(j).

IV. Time

In computing any period of time prescribed or allowed by this CAP, all days referred to shall be calendar days. 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 which is not one of the aforementioned days.

V. Corrective Action Obligations

The Practice agrees to the following:

A. Security Management Process

1. Risk Analysis

a. The Practice shall conduct an accurate and thorough assessment ("Risk Analysis") of the potential security risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information ("ePHI") created, received, maintained or transmitted by the Practice or on its behalf. The Risk Analysis shall incorporate the Practice's facilities, whether owned or rented, and evaluate the risks to the ePHI on its electronic equipment, data systems, and applications controlled, administered or owned by the Practice that contain store, transmit, or receive ePHI. Prior to conducting the

Risk Analysis, the Practice shall develop a complete inventory of all its categories of electronic equipment, data systems, and applications that contain or store ePHI, which will then be incorporated into its Risk Analysis. Within ninety (90) days of the Effective Date, the Practice shall submit the Risk Analysis to HHS for review and approval.

b. Upon receiving notice from HHS specifying any required change to the Risk Analysis, the Practice shall have sixty (60) days in which to revise its Risk Analysis accordingly, and then shall continue to make such revisions until HHS approves the Risk Analysis.

c. Thereafter, the Practice shall review its Risk Analysis annually (or more frequently, if appropriate) and shall promptly conduct an evaluation, and update the Risk Analysis, as necessary, in response to environmental or operational changes affecting the security of ePHI throughout the Practice. Following any updates to its Risk Analysis, the Practice shall assess whether its existing security measures are sufficient to protect its ePHI, develop a strategy to mitigate any risks to ePHI, and revise policies and procedures, training materials, and implement additional security measures as needed.

1. Risk Management

a. Within ninety (90) days of HHS' final approval of the Risk Analysis conducted pursuant to Section V.A.1 above, the Practice shall provide HHS with a risk management plan that addresses and mitigates the security risks and vulnerabilities identified in the Risk Analysis ("Risk Management Plan") for HHS' review, and either approval or disapproval. The Risk Management Plan shall include a process and timeline for the Practice's implementation, evaluation, and revision of their risk remediation activities.

b. Upon receiving notice from HHS specifying any required changes to the Risk Management Plan, the Practice shall have sixty (60) days to make the required changes accordingly, and then submit the revised Risk Management Plan to HHS for review, and either approval or disapproval. This process shall continue until HHS approves the Risk Management Plan.

c. The Practice shall promptly implement the Risk Management Plan upon HHS' final approval in accordance with the Practice's applicable administrative procedures.

2. Revise Policies and Procedures

1. Security Management Process

a. The Practice shall, to the extent necessary, revise, its current policies and procedures relating to Risk Analysis and the implementation of the Risk Management Plan, as required by Sections V.A.1 and V.A.2, respectively. Such policies and procedures must comply with the HIPAA Rules.

b. Within thirty (30) days of the Effective Date for this CAP, the Practice shall submit the policies and procedures required by paragraph V.B.1.a to HHS for review and approval. Upon receiving any such notice of required revisions to such policies and procedures from HHS, the Practice shall have thirty (30) days in which to revise the policies

and procedures accordingly, and submit the revised policies and procedures to HHS for review and approval. The submission and review process shall continue until HHS approves such policies and procedures.

c. Within thirty (30) days of HHS' approval of the revised policies and procedures required by Section V.B.1.a of this CAP, the Practice shall finalize and officially adopt them in accordance with its applicable administrative procedures.

2. Business Associate Relationships

a. The Practice shall revise its policies and procedures relating to Business Associates to: 1) designate one or more individual(s) who are responsible for ensuring that the Practice enters into a business associate agreement with each of its business associates, as defined by the HIPAA Rules, prior to the Practice disclosing protected health information (PHI) to the business associate; 2) create a process for assessing the Practice's current and future business relationships to determine whether each relationship is with a "business associate," as that term is defined under the HIPAA Rules; 3) create a process for negotiating and entering into business associate agreements with business associates prior to disclosing PHI to the business associates; 4) create a standard template business associate agreement; and 5) create a process for maintaining such documentation of each business associate agreement for at least six (6) years beyond the date of when the business associate relationship is terminated. Such policies and procedures must comply with the HIPAA Rules.

b. Within thirty (30) days of the Effective Date for this CAP, the Practice shall submit the policies and procedures required by Section V.B.2.a to HHS for review and approval. Upon receiving any such notice of required revisions to such policies and procedures from HHS, the Practice shall have thirty (30) days in which to revise the policies and procedures accordingly, and submit the revised policies and procedures to HHS for review and approval. The submission and review process shall continue until HHS approves such policies and procedures.

c. Within thirty (30) days of HHS' approval of the revised policies and procedures required by Section V.B.2.a of this CAP, the Practice shall finalize and officially adopt them in accordance with its applicable administrative procedures.

d. Within thirty (30) days of HHS' approval of the revised policies and procedures required by Section V.B.2.a of this CAP, the Practice shall provide OCR a copy of the business associate agreement that the Practice entered into with Dr. Porter's electronic health record (EHR) company(ies).

3. Uses and Disclosures of PHI

a. The Practice shall revise its policies and procedures relating to uses and disclosures of PHI to ensure that its workforce members understand: 1) the circumstances under which the Practice may use and disclose PHI; 2) how to identify situations that constitute impermissible uses and disclosures of PHI; 3) how and when to report situations that might constitute impermissible uses and/or disclosures of PHI to the Practice's Privacy and/or Security Officer; and 4) the guidelines for the use of business associate services and

applications. The Practice's policy shall also include procedures for effective oversight and supervision of members of its workforce members to ensure their compliance with the policy. Such policies and procedures must comply with the HIPAA Rules.

b. Within thirty (30) days of the Effective Date for this CAP, the Practice shall submit the policies and procedures required by paragraph V.B.3.a to HHS for review and approval. Upon receiving any such notice of required revisions to such policies and procedures from HHS, the Practice shall have thirty (30) days in which to revise the policies and procedures accordingly, and submit the revised policies and procedures to HHS for review and approval. The submission and review process shall continue until HHS approves such policies and procedures

c. Within thirty (30) days of HHS' approval of the revised policies and procedures required by Section V.B.3.a of this CAP, the Practice shall finalize and officially adopt them in accordance with its applicable administrative procedures.

3. Training

1. Within ninety (90) days of HHS' final approval of the Practice's revised HIPAA Policies and Procedures required in Sections V.B.1 through V.B.3 of this CAP, the Practice shall forward its proposed training materials on its revised policies and procedures for purposes of compliance with Section C.3 below, to HHS for review and approval. The Practice's training materials shall include privacy and security awareness training related to: a) use of business associate services and applications; and b) disclosures to business associates that require a business associates agreement or other reasonable assurances in place to ensure that the business associate will safeguard the PHI and/or the ePHI.

2. Upon reviewing any required revisions to the training materials from HHS, the Practice shall have thirty (30) days in which to revise the training materials, and then submit the revised training materials to HHS' for review and approval.

3. Within sixty (60) days of HHS' approval of the training materials, the Practice shall ensure that: a) all workforce members who use or disclose PHI have received such training; b) these workforce members will continue to receive such training annually; and c) the Practice will provide each of its new workforce members such training within fifteen (15) days of beginning work at the Practice.

4. The Practice shall review the training materials annually, and, where appropriate, update the training to reflect changes in Federal law or HHS guidance, any issues discovered during audits or reviews, and any other relevant developments.

4. Reportable Events

1. During the Compliance Term, the Practice shall, upon receiving information that a workforce member may have failed to comply with its policies and procedures addressing the requirements of the HIPAA Rules, promptly investigate the matter. If the Practice, after review and investigation, determines that a workforce member has failed to comply with them, the Practice shall report such events to HHS as provided in Section VI.B.3. Such

violations shall be known as Reportable Events. The report to HHS shall include the following:

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

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

2. If no Reportable Events occur during the Compliance Term, the Practice shall so inform HHS in the Annual Report as specified in VI below.

VI. Implementation Report and Annual Reports

A. Implementation Report. Within one hundred and twenty (120) days after HHS approves the Risk Management Plan, specified in Section V.A.2.c above, the Practice shall submit a written report with the documentation described below to HHS for review and approval ("Implementation Report"). The Implementation Report shall include:

1. An attestation signed by an officer of the Practice attesting that the Risk Management Plan is being implemented, and documentation indicating the date of implementation.

2. An attestation signed by an officer of the Practice attesting that its policies and procedures in Section V.B.1 through V.B.3 are being implemented, and the date of implementation.

3. An attestation signed by an officer of the Practice attesting that the Practice has all required business associate agreements in place with its business associates, including Dr. Porter's EHR company(ies).

4. An attestation signed by an officer of the Practice attesting that all required members of the workforce have participated in the training required in Section V.C.3.

5. An attestation signed by an officer of the Practice 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.

B. Annual Reports. The one-year period after the Effective Date and each subsequent one-year period during the course of the Compliance Term shall be known as a "Reporting Period." Within sixty (60) days after the close of each corresponding Reporting Period, the Practice shall submit a report or reports to HHS regarding the Practice's compliance with this CAP for each corresponding Reporting Period ("Annual Report"). The Annual Report shall include:

A copy of the schedule, topic outline, and training materials for the training programs provided during the Reporting Period that is the subject of the Annual Report;

1. An attestation signed by the officer of the Practice attesting that the Practice is obtaining and maintaining written or electronic training certifications from all persons who are required to attend training under this CAP;
2. An attestation signed by an officer of the Practice attesting that any revision(s) to the policies and procedures required by Section V.B were finalized and adopted within thirty (30) days of HHS' approval of the revision(s), which shall include a statement affirming that the Practice distributed the revised policies and procedures to all appropriate members of the Practice's workforce within sixty (60) days of HHS' approval of the revision(s); and
3. A summary of Reportable Events, if any, the status of any corrective and preventative action(s) relating to all such Reportable Events, or an attestation signed by an officer of the Practice stating that no Reportable Events occurred during the Compliance Term.

VII. Document Retention

The Practice shall maintain for inspection and copying, and shall provide to HHS, upon request, all documents and records relating to compliance with this CAP for six (6) years from the Effective Date.

VIII. Breach Provisions

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

A. Timely Written Requests for Extensions.

The Practice may, in advance of any due date set forth 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 five (5) days prior to the date such an act is required or due to be performed. This requirement may be waived by HHS only.

B. Notice of Breach of this CAP and Intent to Impose Civil Monetary Penalty.

The parties agree that a breach of this CAP by the Practice constitutes a breach of the Agreement. Upon a determination by HHS that the Practice has breached this CAP, HHS may notify the Practice's Contact of: (1) the Practice's breach; and (2) HHS' intent to impose a Civil Money Penalty (CMP) pursuant to 45 C.F.R. Part 160, or other remedies for the Covered Conduct set forth in paragraph I.2 of the Agreement and any other conduct that constitutes a violation of the HIPAA Privacy, Security, or Breach Notification Rules ("Notice of Breach and Intent to Impose CMP").

C. The Practice's Response.

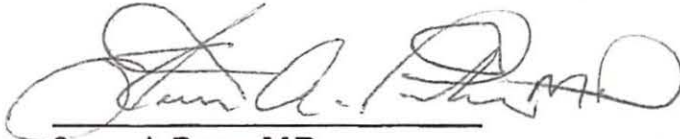
The Practice shall have thirty (30) days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS' satisfaction that:

1. The Practice is in compliance with the obligations of the 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 thirty (30) day period, but that: (a) the Practice has begun to take action to cure the breach; (b) the Practice is pursuing such action with due diligence; and (c) the Practice has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP.

If at the conclusion of the thirty (30) day period, the Practice fails to meet the requirements of Section VIII.C of this CAP to HHS' satisfaction, HHS may proceed with the imposition of a CMP against the Practice pursuant to 45 C.F.R. Part 160 for any violations of the HIPAA Rules applicable to the Covered Conduct set forth in paragraph I.2 of the Agreement and for any other act or failure to act that constitutes a violation of the HIPAA Rules. HHS shall notify the Practice's Contact in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. Part 160.

For Steven A. Porter, M.D., P.C.



Steven A. Porter, M.D.
1508 E. Skyline Drive, Suite 600
Ogden, Utah 84405

2/26/20
Date

For Department of Health and Human Services



Andrea Oliver
Regional Manager, Rocky Mountain Region
Office for Civil Rights

2/26/20
Date