

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 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).

The Upper San Juan Health Service District d/b/a Pagosa Springs Medical Center (PSMC), is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. PSMC is a critical access hospital with 11 inpatient beds, 24-hour emergency care, imaging, and other basic outpatient services, including a primary care clinic, radiology department, surgery department, orthopedics, infusion services, women’s health services, and sports medicine.

HHS and PSMC shall together be referred to herein as the “Parties.”

2. Factual Background and Covered Conduct.

On June 7, 2013, HHS initiated a complaint investigation to determine whether PSMC was in compliance with the HIPAA Rules. HHS’s investigation indicated that the following covered conduct (“Covered Conduct”) occurred:

- A. PSMC impermissibly disclosed the PHI of at least 557 individuals to a former employee on July 8 and September 10, 2013 because it failed to de-activate the former employee’s username and password following termination of employment. *See* 45 C.F.R. § 164.502(a).
- B. PSMC impermissibly disclosed the PHI of at least 557 individuals to Google, its business associate, without obtaining satisfactory assurances from Google, in the form of a written BAA, that Google would appropriately safeguard the PHI. *See* 45 C.F.R. § 164.502(a).

3. No Admission. This Agreement is not an admission of liability by PSMC.

4. No Concession. This Agreement is not a concession by HHS that PSMC 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 Number: 13-161033 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 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

6. **Payment.** HHS has agreed to accept, and PSMC has agreed to pay HHS, the amount of \$111,400 ("Resolution Amount"). PSMC agrees to pay the Resolution Amount on the Effective Date of this Agreement as defined in Paragraph II.14 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

7. **Corrective Action Plan.** PSMC 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 PSMC breaches the CAP, and fails to cure the breach as set forth in the CAP, then PSMC 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 of and conditioned upon PSMC's performance of its obligations under this Agreement, HHS releases PSMC from any actions it may have against PSMC 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 PSMC 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 U.S.C. § 1320d-6.

9. **Agreement by Released Parties.** PSMC shall not contest the validity of its obligation to pay, nor the amount of, the Resolution Amount or any other obligations agreed to under this Agreement. PSMC 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 PSMC 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 or by 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 (6) 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, PSMC agrees that the time between the

Effective Date of this Agreement (as set forth in Paragraph 14) and the date the Agreement may be terminated by reason of PSMC'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. PSMC 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 I.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. In addition, HHS may be required to disclose material related to this Agreement 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.

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 PSMC represent and warrant that they are authorized by PSMC 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 Pagosa Springs Medical Center

Rhonda P. Webb, MD

Dr. Rhonda P. Webb
Chief Executive Officer
Pagosa Springs Medical Center

11/2/18

Date

For the United States Department of Health and Human Services

Andrea Oliver

Andrea Oliver
Office for Civil Rights, Rocky Mountain Region
U.S. Department of Health and Human Services

11/5/18

Date

APPENDIX A
CORRECTIVE ACTION PLAN
BETWEEN THE
DEPARTMENT OF HEALTH AND HUMAN SERVICES
AND
UPPER SAN JUAN HEALTH SERVICE DISTRICT d/b/a PAGOSA SPRINGS MEDICAL CENTER

I. Preamble

Upper San Juan Health Service District d/b/a Pagosa Springs Medical Center (PSMC) 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, PSMC is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. PSMC 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

PSMC 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:

Anita L. Hooton, CHC
Director of Clinical Value/ Privacy Officer
Upper San Juan Health Services District
d/b/a Pagosa Springs Medical Center
95 Pagosa Springs Boulevard
Pagosa Springs, Colorado 81147
Voice: (970) 507-3809
Fax: (970) 731-3707
Email: Anita.Hooton@psmedicalcenter.org

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

Andrea Oliver, Regional Manager
Office for Civil Rights, Rocky Mountain Region
1961 Stout Street, Room 08.148
Denver, Colorado 80294
Voice: (303) 844-7915
Fax: (303) 844-2025
Email: Andrea.Oliver@hhs.gov

PSMC 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, electronic 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 PSMC under this CAP shall begin on the Effective Date of this CAP and end two years (2) years from the Effective Date, unless HHS has notified PSMC under Section VIII hereof of its determination that PSMC breached this CAP. In the event of such a notification by HHS under Section VIII hereof, the Compliance Term shall not end until HHS notifies PSMC that it has determined that the breach has been cured. After the Compliance Term ends, PSMC 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 PSMC’s obligation to comply with the document retention requirements in 45 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

PSMC agrees to the following:

A. Revise Policies and Procedures

1. Business Associate Relationships

a. PSMC shall revise its policies and procedures relating to Business Associates (“Business Associate Policies and Procedures) to: 1) designate one or more individual(s) who are responsible for ensuring that PSMC enters into a business associate agreement with each of its business associates, as defined by the HIPAA Rules, prior to PSMC disclosing protected health information (PHI) to the business associate; 2) create a process for assessing PSMC’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; 5) create a process for maintaining documentation of each business associate agreement for at least six (6) years beyond the date of when the business associate relationship is terminated; and 6) create a

process to limit disclosures of PHI to business associates to the minimum necessary amount of PHI that is reasonably necessary for business associates to perform their duties.

b. Within sixty (60) days of the Effective Date, PSMC shall forward the revised Business Associate Policies and Procedures required by Section V.A.1.a. of this CAP to HHS for its review and approval. Upon receiving any required revisions to such Business Associate Policies and Procedures from HHS, PSMC shall have thirty (30) days to revise them accordingly, and then submit the revised Business Associate Policies and Procedures to HHS for review and approval. This process shall continue until HHS approves the policies and procedures.

c. Within sixty (60) days of HHS' approval of the revised Business Associate Policies and Procedures required by Section V.A.1.a. of this CAP, PSMC shall finalize and officially adopt them in accordance with its applicable administrative procedures. PSMC shall also review its existing business associate agreements for compliance with the HIPAA Rules and its revised Business Associate Policies and Procedures and make any modifications necessary to ensure conformance.

2. Uses and Disclosures of PHI

a. PSMC shall revise its policies and procedures relating to uses and disclosures of PHI (Uses and Disclosures of PII Policies and Procedures) to ensure that its workforce members also understand: 1) how to identify situations that constitute impermissible uses and disclosures of PHI; 2) how and when to report situations that might constitute impermissible uses and/or disclosures of PHI to PSMC's Privacy and/or Security Officer; and 3) the guidelines for the downloading and use of third party services and applications. PSMC'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 oversight may include, training, ongoing privacy and security awareness, and sanctions for non-compliance.

b. Within sixty (60) days of the Effective Date, PSMC shall forward the revised Uses and Disclosures of PHI Policies and Procedures required by Section V.A.2.a. of this CAP to HHS for its review and approval. Upon receiving any required revisions to such Uses and Disclosures of PHI Policies and Procedures from HHS, PSMC shall have thirty (30) days to revise them accordingly, and then submit the revised Uses and Disclosures of PHI Policies and Procedures to HHS for review and approval. This process shall continue until HHS approves the policies and procedures.

c. Within sixty (60) days of HHS' approval of the revised Uses and Disclosures of PHI Policies and Procedures required by Section V.A.2.a. of this CAP, PSMC shall finalize and officially adopt them in accordance with its applicable administrative procedures.

B. Security Management Process

1. Risk Analysis

a. PSMC shall develop a current, comprehensive and thorough risk analysis of security risks and vulnerabilities include the electronic protected health information (ePHI) created, received, maintained or transmitted by PSMC or on its behalf ("Risk Analysis"). Within ninety (90) days of the Effective Date, PSMC 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, PSMC shall have sixty (60) days in which to revise its Risk Analysis accordingly, and then submit the revised Risk Analysis to HHS for review, and approval or disapproval. This process shall continue until HHS approves the Risk Analysis.

c. Thereafter, PSMC 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 PSMC. Following any updates to its Risk Analysis, PSMC 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.

2. Risk Management

a. Within ninety (90) days of HHS' final approval of the Risk Analysis conducted pursuant to Section V.B.1 above, PSMC 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 PSMC's implementation, evaluation, and revision of its risk remediation activities.

b. Upon receiving notice from HHS specifying any required changes to the Risk Management Plan, PSMC 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. PSMC shall promptly implement the Risk Management Plan upon HHS' final approval in accordance with PSMC's applicable administrative procedures.

C. Training

1. Within sixty (60) days of HHS' approval of any revised policies and procedures required by Sections V.A.1.a. and V.A.2.a. of this CAP, PSMC shall forward its proposed training materials on the revised policies and procedures for purposes of compliance with C.3 below, to HHS for review and approval. PSMC's training materials shall include privacy and security awareness related to: a) use of third-party services and applications; b) disclosures to third party entities that require a business associate agreement or other reasonable assurance in place to ensure that the business associate will safeguard the PHI and/or ePHI; c) security incident reporting; and d) password management. The training materials shall also include, for supervisors and other responsible officials, effective oversight of workforce members' uses and disclosures of PHI, including ePHI to ensure the workforce members' compliance with the HIPAA Rules and PSMC's internal policies and procedures.

2. Upon receiving any required revisions to the training materials from HHS, PSMC 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, PSMC shall provide documentation that a) all workforce members who use or disclose PHI have received such training, b) that

these workforce members will continue to receive such training annually, and c) that each new PSMC workforce member will receive such training within fifteen (15) days of beginning work at PSMC.

4. PSMC 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.

D. Reportable Events

1. During the Compliance Term, PSMC 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 PSMC, after review and investigation, determines that a workforce member has failed to comply with them, PSMC shall report such events to HHS as provided in Section VI.B.4. 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 PSMC's Privacy, Security, and Breach Notification policies and procedures; and

b. A description of the actions taken and any further steps PSMC 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 its Privacy, Security, and Breach Notification policies and procedures.

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

VI. Implementation Report and Annual Reports

A. **Implementation Report.** Within one hundred twenty (120) days after HHS approves the Risk Management Plan, specified in Section V.B.2.c. above, PSMC 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 PSMC attesting that the Risk Management Plan is being implemented, and documentation indicating the date of implementation.

2. An attestation signed by an officer of PSMC attesting that its Business Associate and Uses and Disclosures Policies and Procedures are being implemented, and the date of implementation.

3. An attestation signed by an officer of PSMC attesting that PSMC has all required business associate agreements in place with its business associates.

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

5. An attestation signed by an officer of PSMC 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 beginning on the Effective Date and each subsequent one-year period during the course of the period of compliance obligations shall be referred to as “the Reporting Periods.” PSMC shall submit to HHS Annual Reports with respect to the status of and findings regarding PSMC’s compliance with this CAP for each of the two (2) Reporting Periods. PSMC shall submit each Annual Report to HHS no later than thirty (30) days after the end of each corresponding Reporting Period. The Annual Report shall include:

1. A detailed description of any updates or changes, to the Risk Analysis or Risk Management Plan made pursuant to Section V.B.1 and V.B.2. This shall include a summary of PSMC’s strategy related to the assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by PSMC; the identification of all outside entities assisting PSMC in this process; and documentation related to the security measures PSMC has implemented or is implementing to sufficiently reduce the identified risks and vulnerabilities to a reasonable and appropriate level;

2. A detailed description of any revisions to PSMC’s Business Associate Policies and Procedures and/or Uses and Disclosures of PHI Policies and Procedures;

3. A summary of Reportable Events defined in Section V.D, if any, identified during the Reporting Period and the status of any corrective and preventative action relating to all such Reportable Events; and

4. An attestation signed by an officer of PSMC attesting that he or she has reviewed the Annual Report, has made a reasonable inquiry regarding its content and believes that, upon such inquiry, the information is accurate and truthful.

VII. Document Retention

PSMC 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

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

A. Timely Written Requests for Extensions

PSMC 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.

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

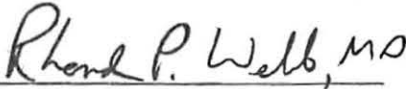
The parties agree that a breach of this CAP by PSMC constitutes a breach of the Agreement. Upon a determination by HHS that PSMC has breached this CAP, HHS may notify PSMC of: (1) PSMC’s breach; and (2) HHS’ intent to impose a CMP pursuant to 45 C.F.R. Part 160, or other remedies for the Covered Conduct 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. PSMC's Response. PSMC 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. PSMC 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 30-day period, but that: (a) PSMC has begun to take action to cure the breach; (b) PSMC is pursuing such action with due diligence; and (c) PSMC has provided to HHS a reasonable timetable for curing the breach.


D. Imposition of CMP. If at the conclusion of the 30-day period, PSMC 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 PSMC pursuant to 45 C.F.R. Part 160 for any violations of 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 PSMC in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. Part 160.

For Pagosa Springs Medical Center


Dr. Rhonda P. Webb
Chief Executive Officer
Pagosa Springs Medical Center

11/2/18
Date

For United States Department of Health and Human Services


Andrea Oliver
Regional Manager
Office for Civil Rights, Rocky Mountain Region
U.S. Department of Health and Human Services

11/5/18
Date