

## **RESOLUTION AGREEMENT**

### **I. Recitals**

1. **Parties.** The Parties to this Resolution Agreement (“Agreement”) are the United States Department of Health and Human Services, Office for Civil Rights (“HHS”) and the Trustees of Columbia University in the City of New York (“CU”). HHS and CU shall together be referred to herein as the “Parties.”

2. **Factual Background and Covered Conduct**

On September 27, 2010, the HHS Office for Civil Rights received notification from “New York-Presbyterian Hospital and Columbia Medical Center” regarding a breach of unsecured electronic protected health information (ePHI). On November 5, 2010, HHS notified CU of HHS’ investigation regarding CU’s compliance with the Privacy and Security Rules promulgated by HHS pursuant to the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub.L. 104-191, 110 Stat. 1936.

HHS’ investigation indicated that the following conduct occurred (“Covered Conduct”):

a. CU failed to conduct an accurate, and thorough risk analysis that incorporates all IT equipment, applications and data systems utilizing ePHI, including the server accessing NYP-ePHI.

b. CU failed to implement processes for assessing and monitoring IT equipment, applications and data systems that were linked to NYP patient data bases prior to the breach incident and failed to implement security measures sufficient to reduce the risks of inappropriate disclosure to an acceptable level.

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

4. **No Concession.** This Agreement is not a concession by HHS that CU is not in violation of the HIPAA Privacy and Security Rules and that CU is not liable for civil money penalties.

5. **Intention of Parties to Effect Resolution.** This Agreement is intended to resolve the HHS Complaint No. 13-163170, regarding possible violations of the HIPAA Privacy and Security Rules. In consideration of the Parties’ interest in avoiding the uncertainty, burden, and expense of further investigation and formal proceedings, the Parties agree to resolve these matters according to the terms and conditions below.

### **II. Terms and Conditions**

6. **Payment.** CU agrees to pay HHS the amount of one million five hundred thousand dollars (\$1,500,000.00)(“Resolution Amount”). CU agrees to pay the Resolution

Amount on the Effective Date of this Agreement as defined in paragraph 14 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

7. **Corrective Action Plan.** CU 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 CU breaches the CAP, then CU will be in breach of this Agreement and HHS will not be subject to the Release set forth in paragraph 8 of this Agreement.

8. **Release by HHS.** In consideration and conditioned upon CU's performance of its obligations under this Agreement, HHS releases CU from any actions it has or may have against CU under the Privacy and Security Rules arising out of or related to the Covered Conduct identified in paragraph 2. HHS does not release CU from, nor waive any rights, obligations, or causes of action other than those specifically 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.** CU 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. CU 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 CU and its successors, 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. 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 both 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 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, CU agrees that the time between the Effective Date of this Agreement and the date this Resolution Agreement may be terminated by reason of CU'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. CU 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 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 Resolution Agreement.

16. **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.

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 CU represent and warrant that they are authorized to execute this Agreement. The individual(s) signing this Agreement on behalf of HHS represents and warrants that he/she is signing this Agreement in his/her official capacities and that he/she is authorized to execute this Agreement.

**For The Trustees of Columbia University in the City of New York**

/s/

\_\_\_\_\_  
Mark McDougle  
Senior Vice President and Chief Operating Officer  
Columbia University Medical Center

\_\_\_\_\_  
Date

**For the United States Department of Health and Human Services**

/s/

\_\_\_\_\_  
Linda C. Colón  
Regional Manager, Region II  
Office for Civil Rights

\_\_\_\_\_  
Date

## Appendix A

### CORRECTIVE ACTION PLAN

#### BETWEEN

#### THE UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES AND THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK

#### I. Preamble

The Trustees of Columbia University in the City of New York (CU) 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, CU is entering into a Resolution Agreement (Agreement) with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. CU enters into this CAP as consideration for the release set forth in paragraph 8 of the Agreement.

#### II. Contact Persons and Submissions

##### A. Contact Persons

CU has identified the following individual as its contact person regarding the implementation of this CAP and for receipt and submission of notifications and reports:

Robert V. Sideli, MD  
Chief Information Officer, Columbia University Medical Center  
630 W. 168<sup>th</sup> Street  
New York, NY 10032  
Telephone: 212-305-6776  
[Rvs1@columbia.edu](mailto:Rvs1@columbia.edu)

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

Linda C. Colón, Regional Manager, Region II  
Office for Civil Rights  
U.S. Department of Health and Human Services  
26 Federal Plaza, Suite 3312  
New York, New York 10278  
Voice Phone (212) 264-4136  
Fax: (212) 264-3039  
[Linda.Colon@HHS.gov](mailto:Linda.Colon@HHS.gov)

CU 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 for this CAP shall be calculated in accordance with paragraph 14 of the Agreement (Effective Date). The period for compliance with the obligations assumed by CU under this CAP shall begin on the Effective Date of this CAP and end three (3) years from the date (“Compliance Term”). Except that after the Compliance Term ends, CU shall still be obligated to: (a) submit the Annual Report for the final Reporting Period, as set forth in section VI.C.; and (b) comply with the document retention requirement set forth 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 which is not one of the aforementioned days.

**V. Corrective Action Obligations**

CU agrees to take the following corrective actions to address the Covered Conduct. To the extent necessary, CU shall collaborate with New York-Presbyterian (NYP) for the purpose of implementing the actions specified below:

A. Conduct a thorough Risk Analysis

Within one hundred eighty (180) calendar days of the Effective Date, CU shall conduct a comprehensive and thorough risk analysis of security risks and vulnerabilities that incorporates all electronic equipment, data systems and applications controlled, administered or owned by CU, its workforce members that contains, stores, transmits or receives CU ePHI. CU shall develop a complete inventory of all electronic equipment, data systems, and applications that contain or store ePHI which will then be incorporated in its Risk Analysis.

B. Develop and Implement a Risk Management Plan

1. Within ninety (90) calendar days of completion of the risk analysis specified in Section V.A, CU shall develop an organization wide risk management plan to address and mitigate any security risks and vulnerabilities found in its risk analysis. The plan shall include a process and timeline for implementation, evaluation, and revision. The plan shall be forwarded to HHS for its review consistent with paragraph 2 below.
2. HHS shall review and recommend changes to the plan. Upon receiving HHS' recommended changes, CU shall have sixty (60) calendar days to provide a revised plan. CU shall begin implementation of the plan and distribute to workforce members involved with implementation of the plan within ninety (90) calendar days of HHS' approval.

C. Review and Revise Policies and Procedures on Information Access Management

1. Within ninety (90) calendar days of the Effective Date, CU shall review and to the extent necessary revise its internal policies and procedures for authorizing access to CU ePHI. The revised policies and procedures shall include a process to be followed by workforce members for requesting authorization to access CU ePHI (including criteria for granting such access), obtaining approval of such request, documenting such request, and conducting periodic monitoring of ePHI usage. CU shall forward its policies and procedures for authorizing access to all CU ePHI to HHS for its review consistent with paragraph 2 below.
2. HHS shall review and recommend changes to the policies and procedure specified in paragraph 1. Upon receiving HHS' recommended changes, CU shall have sixty (60) calendar days to provide revised policies and procedure to HHS for review and approval. CU shall implement its policies and procedure and distribute to affected workforce members within ninety (90) calendar days of HHS' approval.

D. Compliance with Evaluation Standard

1. Within one hundred twenty (120) calendar days of the Effective date, CU shall develop a process to evaluate any environmental or operational changes that affect the security of CU ePHI.
2. HHS shall review and recommend changes to the process specified in paragraph 1. Upon receiving HHS' recommended changes, CU shall have sixty (60) calendar days to provide revised policies and procedure to HHS for review and approval. CU shall implement its process including distributing to workforce members with responsibility for performing such evaluations within ninety (90) calendar days of HHS' approval.

E. Review and Revise Policies and Procedures on Device and Media Controls

1. Within ninety (90) calendar days of the Effective Date, CU shall review and to the extent necessary, revise its policies and procedures related to the use of hardware and electronic media including, but not limited to laptops, servers, tablets, mobile phones, USB drives, external hard drives, DVDs and CDs that may be used to access, store, download or transmit CU ePHI. The revised policies shall identify criteria for the use of such hardware and electronic media and procedures for obtaining authorization for the use of personal devices and media that utilized CU ePHI systems. The policies shall also address security responsibilities, including disposal and reuse of personal devices and media and regular compliance monitoring. CU shall forward its policies and procedures to HHS for its review consistent with paragraph 2 below.
2. HHS shall review and recommend changes to the policies and procedure specified in paragraph 1. Upon receiving HHS' recommended changes, CU shall have sixty (60) calendar days to provide revised policies and procedure to HHS for review and approval. CU shall implement its policies and procedure and distribute to affected workforce members who have access to ePHI within ninety (90) calendar days of HHS' approval.

F. Develop a Privacy and Security Awareness Training Program

1. Within ninety (90) calendar days of the Effective Date, CU shall develop a mandatory Health Information Privacy and Security Awareness Training Program (the Training Program) for workforce members that have access to protected health information including ePHI. The Training Program shall include instruction on compliance with the HIPAA Privacy, Security, and Breach Notification Rules and CU health information security policies and procedures, and shall particularly include training on the policies and procedures developed as required by Section V.C-E of this CAP.
2. Under the Training Program, CU shall provide training to all workforce members as soon as possible but no later than one year of the Effective Date and yearly thereafter. Any workforce member that commence working for CU after the development of the Training Program shall be trained within thirty (30) calendar days of the commencement of their employment with CU.
3. Each individual who is required to attend training shall certify, in writing or in electronic form, that he or she has received the required training and the date training was received. CU shall retain copies of such certifications for no less than six years following the date training was provided.
4. CU shall review the Training Program, including all training materials developed as part of the program, 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.

## **VI. Implementation Report and Annual Reports**

### **A. Reportable Events.**

1. The one-year period beginning on the Effective Date and each following one-year period during the course of the period of compliance obligations shall be referred to as “the Reporting Periods.” During each Reporting Period under this CAP, CU shall, upon receiving information that a workforce member may have failed to comply with its Privacy, Security, and Breach Notification policies and procedures, promptly investigate the matter. If CU, after review and investigation, determines that a member of the workforce of a covered health care component has failed to comply with its Privacy, Security and Breach Notification policies and procedures, CU shall notify HHS in writing within 30 days. 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 provision(s) of CU Privacy, Security, and Breach Notification policies and procedures implicated; and
  - b. A description of the actions taken and any further steps CU plans to take to address the matter, to mitigate any harm, and to prevent it from recurring, including the application of appropriate sanctions against covered health care component workforce members who failed to comply with its Privacy, Security, and Breach Notification policies and procedures.
  - c. If no Reportable Events have occurred within a Reporting Period, CU shall so inform HHS in its Annual Report for that Reporting Period in accordance with section VI.C of this CAP.

### **B. Implementation Report.** Within two hundred and ten (210) calendar days after receiving HHS’ approval of the documents required under Section V, above, CU shall submit a written report to HHS summarizing the status of its implementation of the obligations of this CAP (“Implementation Report”). The Implementation Report shall include:

1. An attestation signed by an officer of CU attesting that the Plan and Policies and Procedures required by Section V (a) have been adopted; (b) are being implemented; (c) have been distributed to all appropriate members of the workforce;

2. A copy of all training materials used for the training required by this CAP, a description of the training, including a summary of the topics covered, the length of the session(s) and a schedule of when the training session(s) were held;
  3. An attestation signed by an officer of CU attesting that all members of its workforce identified in paragraph V. F. 1 have completed the initial training required by this CAP and have executed the training certifications required by paragraph V.F.3.;
  4. An attestation signed by an officer of CU listing all of CU's locations, the name under which each location is doing business, the corresponding mailing address, phone number and fax number for each location, and attesting that each location has complied with the obligations of this CAP; and
  5. An attestation signed by an officer of CU 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.
- C. 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 60 days after each corresponding Reporting Period, CU shall annually submit a report to HHS regarding CU's compliance with this CAP for each Reporting Period ("Annual Report"). The Annual Report shall include:
1. 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;
  2. An attestation signed by an officer of CU attesting that CU obtains and maintains written or electronic training certifications from all persons who are required to attend training under this CAP;
  3. A summary of Reportable Events identified during the Reporting Period and the status of any corrective and preventative action(s) relating to all such Reportable Events.

## **VII. Document Retention**

CU shall maintain for HHS inspection and copying all documents and records relating to compliance with this CAP for six (6) years.

## **VIII. Breach Provisions**

CU is expected to fully and timely comply with all provisions of its CAP obligations.

A. Timely Written Requests for Extensions

CU 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 or file any notification or report required by this CAP. A “timely written request” is defined as a request in writing received by HHS at least five (5) business 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 CU constitutes a breach of the Agreement. Upon a determination by HHS that CU has breached this CAP, HHS may notify CU of: (a) CU’s breach; and (b) HHS’ intent to impose a CMP pursuant to 45 C.F.R. Part 160 for the Covered Conduct set forth in paragraph 2 of the Agreement and for any other conduct that constitutes a violation of the HIPAA Privacy and Security Rules (Notice of Breach and Intent to Impose CMP).

C. CU’s Response.

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

1. CU is in compliance with the obligations of the CAP cited by HHS as being 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:
  - (i) CU has begun to take action to cure the breach;
  - (ii) CU is pursuing such action with due diligence; and
  - (iii) CU has provided to HHS a reasonable timetable for curing the breach.

D. Imposition of CMP.

If at the conclusion of the 30-day period, CU fails to meet the requirements of section VII.C to HHS’ satisfaction, HHS may proceed with the imposition of a CMP against CU pursuant to 45 C.F.R. Part 160 for the Covered Conduct set forth in paragraph 2 of the Agreement and for any other conduct that constitutes a violation of the HIPAA Privacy, Security, and Breach Notification Rules. HHS shall notify CU in writing of its determination to proceed with the imposition of a CMP.

**For The Trustees of Columbia University in the City of New York**

/s/

\_\_\_\_\_  
Mark McDougle  
Senior Vice President and Chief Operating Officer  
Columbia University Medical Center

\_\_\_\_\_  
Date

**For the United States Department of Health and Human Services**

/s/

\_\_\_\_\_  
Linda C. Colón  
Regional Manager, Region II  
Office for Civil Rights

\_\_\_\_\_  
Date