

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 45 C.F.R. 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 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 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. The University of Massachusetts Amherst (“UMass”) which is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore is required to comply with the HIPAA Rules. UMass is a hybrid entity, as defined at 45 C.F.R. § 164.103, that has designated the following components as its covered health care component (hereinafter referred to as “health care component”): the Center for Language, Speech and Hearing (hereinafter referred to as “the Center”); the Center for Counseling and Psychological Health; the Psychological Services Center; the Student Health Benefit Plan; University Health Services; and the following UMass departments only to the extent to which they perform business associate functions within UMass: UMass Information Technology, Administration & Finance, Facilities/Plant Management, and Office of the General Counsel.
- C. HHS and UMass shall together be referred to herein as the “Parties.”

2. **Factual Background and Covered Conduct.**

On June 4, 2013, HHS received notification from UMass regarding a workstation at the Center that was infected by malware, which may have resulted in a breach of unsecured electronic protected health information (“ePHI”) affecting approximately 1,670 individuals. On August 27, 2013, HHS notified UMass of its investigation regarding UMass’ compliance with the Privacy, Security and Breach Notification Rules. HHS’ investigation indicated that the following conduct occurred (“Covered Conduct”):

- A. UMass failed to include each component that would meet the definition of a covered entity or business associate if it were a separate legal entity in its

hybrid entity designation and had UMass did not implement policies and procedures at the Center to ensure compliance with the HIPAA Privacy and Security Rules (*see 45 C.F.R. § 164.105(a)(2)*).

- B. UMass did not conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of its ePHI (*see 45 C.F.R. § 164.308 (a)(1)(ii)(A)*).
- C. UMass did not implement technical security measures at the Center to guard against unauthorized access to ePHI that is transmitted over an electronic communications network by ensuring that firewalls were in place (*see 45 C.F.R. § 164.312(e)*).
- D. UMass provided access to the ePHI of 1,670 individuals whose information was maintained on a workstation at the Center that was infected by malware, in violation of the Privacy Rule. (*see 45 C.F.R. § 164.502(a)*).

3. **No Admission.** This Agreement is not an admission, concession, or evidence of liability by UMass or of any fact or any violation of any law, rule, or regulation, including any violation of the HIPAA Rules. This Agreement is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind, and UMass' agreement to undertake any obligation under this Agreement shall not be construed as an admission of any kind.

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

5. **Intention of Parties to Effect Resolution.** This Agreement is intended to resolve HHS Transaction Number: 13-161455 and any potential violations of the HIPAA Rules related to the Covered Conduct specified in section 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 UMass has agreed to pay HHS, the amount of \$650,000 ("Resolution Amount"). UMass agrees to pay the Resolution Amount on the Effective Date of this Agreement as defined in section II.14 by automated clearing house transaction pursuant to written instructions to be provided by HHS.

7. **Corrective Action Plan.** UMass 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 UMass breaches the CAP, and fails to cure the breach as set forth in

the CAP, then UMass will be in breach of this Agreement and HHS will not be subject to the Release set forth in section II.8 of this Agreement.

8. Release by HHS. In consideration of and conditioned upon UMass' performance of its obligations under this Agreement, HHS releases UMass from any actions it may have against UMass under the HIPAA Rules arising out of or related to the Covered Conduct identified in section I.2 of this Agreement. HHS does not release UMass 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 section. 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. UMass 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. UMass 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 UMass 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 civil money penalty ("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, UMass agrees that the time between the Effective Date of this Agreement and the date the Agreement may be terminated by reason of UMass' breach, plus one-year thereafter, will not be included in calculating the six (6) year statute of limitations applicable to the potential violations which are the subject of this Agreement. UMass waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct identified in section 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. With respect to requests for the disclosure of such records, UMass shall retain the interests set forth in 45 C.F.R. § 5.65 to the extent that requested records contain information that constitute trade secrets and/or confidential commercial information and have been designated as exempt from disclosure by UMass.

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 UMass represent and warrant that they are authorized by UMass 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 University of Massachusetts - Amherst

Kumble R. Subbaswamy
Kumble R. Subbaswamy
Chancellor
University of Massachusetts Amherst

11/14/16
Date

For Department of Health and Human Services

Susan Pezzullo Rhodes
Susan M. Pezzullo Rhodes
Regional Manager, New England Region
Office for Civil Rights

11/16/16
Date

Appendix A

CORRECTIVE ACTION PLAN

BETWEEN THE

DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

UNIVERSITY OF MASSACHUSETTS – AMHERST

I. Preamble

The University of Massachusetts Amherst (hereinafter known as “UMass”) 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, UMass is entering into a Resolution Agreement (“Agreement”) with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. UMass enters into this CAP as part of the consideration for the release set forth in section II.8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

UMass 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:

Robert S. Feldman
Deputy Chancellor and Interim Dean, College of Education
University of Massachusetts Amherst
Chancellor's Office
374 Whitmore
181 Presidents Drive
Amherst, MA 01003-9313
Telephone: 413.545.2211
Fax: 413.545.2328
email: feldman@chancellor.umass.edu

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

Susan M. Pezzullo Rhodes
Office for Civil Rights, New England Region
U.S. Department of Health and Human Services
JFK Federal Building, Room 1875

Boston, MA 02203
Telephone: 617-565-1347
Fax: 617-565-3809

UMass 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, secure file transfer 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 section II.14 of the Agreement (“Effective Date”). The period for compliance (“Compliance Term”) with the obligations assumed by UMass 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 UMass under section VIII hereof of its determination that UMass has 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 UMass that it has determined that the breach has been cured or HHS proceeds with the imposition of a CMP against UMass pursuant to 45 C.F.R. Part 160 and section VIII.D. of this CAP. After the Compliance Term ends, UMass shall still be obligated to submit the Implementation Report as required by section VI (if it has not already done so) and comply with the document retention requirement in section VII.

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

UMass agrees to the following:

A. Security Management Process

1. UMass shall conduct a comprehensive and thorough Risk Analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by UMass. This Risk Analysis shall incorporate all UMass facilities, whether owned or rented, and evaluate the risks to the ePHI on all of its electronic equipment, data systems, and applications controlled, administered or owned by

UMass or any UMass entity, that contain, store, transmit, or receive ePHI. Prior to conducting the Risk Analysis, UMass shall develop a complete inventory of all of its facilities, electronic equipment, data systems, and applications that contain or store ePHI that will then be incorporated into its Risk Analysis. UMass may submit a Risk Analysis currently underway for consideration by HHS for compliance with this provision. UMass shall provide documentation supporting a review of current security measures and level of risk to its ePHI associated with the following: network segmentation; network infrastructure; vulnerability scanning; logging and alerts; and patch management.

2. The Contact Person shall provide the Risk Analysis, consistent with section V.A.1, to HHS within one hundred eighty (180) days of the Effective Date for HHS' review. Within sixty (60) days of its receipt of UMass' Risk Analysis, HHS will inform the Contact Person whether HHS approves or disapproves of the Risk Analysis. If HHS disapproves of the Risk Analysis, HHS shall provide the Contact Person with technical assistance, as necessary, regarding the basis for disapproval so that UMass may prepare a revised Risk Analysis. UMass shall have sixty (60) days in which to revise its Risk Analysis accordingly, and then have the Contact Person submit the revised Risk Analysis to HHS for review and approval. This submission and review process shall continue until HHS approves the Risk Analysis.

3. UMass shall develop an enterprise-wide Risk Management Plan to address and mitigate any security risks and vulnerabilities found in the Risk Analysis described above. The Risk Management Plan shall include a process and timeline for UMass' implementation, evaluation, and revision of its risk remediation activities. UMass may submit a Risk Management Plan currently underway for consideration by HHS for compliance with this provision.

4. Within ninety (90) days of HHS' final approval of the Risk Analysis described in section V.A above, the Contact Person shall submit UMass' Risk Management Plan to HHS for HHS' review. Within sixty (60) days of its receipt of UMass' Risk Management Plan, HHS will inform the Contact Person whether HHS approves or disapproves of the Risk Management Plan. If HHS disapproves of the Risk Management Plan, HHS shall provide the Contact Person with technical assistance, as necessary, so that UMass may prepare a revised Risk Management Plan. Upon receiving a letter of disapproval of the Risk Management Plan from HHS and a description of any required changes to the Risk Management Plan, UMass shall have sixty (60) days in which to revise its Risk Management Plan accordingly, and, through the Contact Person, submit the revised Risk Management Plan to HHS for review and approval. This submission and review process shall continue until HHS approves the Risk Management Plan. Within thirty (30) days of HHS' approval of the Risk Management Plan, UMass shall begin implementation of the Risk Management Plan and distribute the plan to workforce members involved with implementation of the plan.

B. Policies and Procedures

1. UMass shall review and revise, as necessary, the Center's written policies and procedures to comply with the Federal standards that govern the privacy of individually

identifiable health information (45 C.F.R. Part 160 and 164, Subparts A, and E of 45 C.F.R. Part 164, the “Privacy Rule”) and the Federal standards for notification in the case of breach of unsecured protected health information (45 C.F.R. Part 160 Subparts A and D of 45 C.F.R. Part 164, the “Breach Notification Rule”).

2. UMass shall provide the policies and procedures identified in section V.B.1 above to HHS for review and approval within ninety (90) days of HHS’ approval of its risk analysis, as required by A.2. Upon receiving any recommended changes to such policies and procedures from HHS, UMass shall have thirty (30) days to revise such policies and procedures accordingly and provide the revised policies and procedures to HHS for review and approval.

3. UMass shall adopt (in accordance with its applicable administrative procedures) the policies and procedures approved by HHS pursuant to section V.B.2 within thirty (30) days of receipt of HHS’ approval.

C. Distribution of Policies and Procedures

1. UMass shall distribute the policies and procedures identified in section V.B. to all members of the Center’s workforce who use or disclose ePHI within thirty (30) days of HHS approval of such policies and procedures, and thereafter to new members of the workforce who will use or disclose ePHI within thirty (30) days of their becoming a member of the workforce.

D. Training

1. All UMass workforce members at the Center who have access to ePHI shall receive specific training on the policies and procedures submitted to HHS under section V.B. within ninety (90) days of the adoption of those policies and procedures in accordance with section V.B.3 and at least annually thereafter. Any individuals who will have access to ePHI that join UMass’ workforce after the initial training period described in this section shall be trained within thirty (30) days of their becoming a member of the workforce at the Center.

2. Each UMass workforce member at the Center who is required to attend training shall certify, in electronic or written form, that he or she has received the training. The training certification shall specify the date training was received. All course materials shall be retained in compliance with section VII.

3. UMass shall review the training at least 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.

E. Reportable Events.

1. During the Compliance Term, in the event that UMass receives information that a workforce member may have failed to comply with the policies and procedures submitted to HHS under section V.B., UMass shall promptly investigate this matter. If UMass determines, after such investigation, that during the Compliance Term a member of its workforce has failed to comply with the policies and procedures submitted to HHS under section V.B., UMass shall

notify HHS in writing within thirty (30) days. Such violations shall be known as Reportable Events. The report to HHS shall include the following information:

- a. A complete description of the event, including the relevant facts, the persons involved, and the provision(s) of the policies and procedures implicated; and
 - b. A description of the actions taken and any further steps UMass plans to take to address the matter to mitigate any harm, and to prevent it from recurring, including application of appropriate sanctions against workforce members who failed to comply with the policies and procedures submitted to HHS under section V.B.
2. If no Reportable Events occur within the Compliance Term, UMass shall so inform HHS in its Implementation Report as specified in section VI below.

VI. Implementation Report

A. Within one-hundred and eighty (180) days after HHS approves Policies and Procedures specified in section V.B. above, UMass 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 UMass attesting that the policies and procedures submitted to HHS under section V.B. have been implemented;
2. An attestation signed by an officer of UMass attesting that all members of the UMass workforce at the Center that use or disclose ePHI have completed training as required by this CAP and have executed the training certifications required by section V.D.2.
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 UMass stating that no Reportable Events occurred during the Compliance Term.
4. An attestation signed by an officer of UMass attesting that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its content and believes, based upon such inquiry, that the information is accurate and truthful.

VII. Document Retention

UMass 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. Nothing in this Agreement shall be construed to constitute a waiver by UMass of any applicable legal privilege against disclosure, including the attorney-client privilege and the work product doctrine. If HHS requests access to information or documentation which UMass seeks to withhold on the basis of an applicable legal privilege against disclosure,

including the attorney-client privilege or the attorney work product doctrine, UMass shall provide HHS with a description of such information and the type of privilege asserted.

VIII. Breach Provisions

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

A. Timely Written Requests for Extensions

UMass 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 Money Penalty (“CMP”)

The Parties agree that a breach of this CAP by UMass constitutes a breach of the Agreement. Upon a determination by HHS that UMass has breached this CAP, HHS may notify UMass of: (1) UMass’ 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 section 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. UMass’ Response. UMass 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. UMass 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) UMass has begun to take action to cure the breach; (b) UMass is pursuing such action with due diligence; and (c) UMass has provided HHS a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the thirty (30) day period, UMass 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 UMass pursuant to 45 C.F.R. Part 160 for any violations of the HIPAA Rules related to the Covered Conduct set forth in section 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 UMass in writing of its determination to proceed with the imposition of a CMP pursuant to 45 C.F.R. §§ 160.312(a)(3)(i) and (ii).

For University of Massachusetts - Amherst

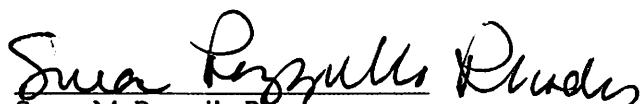


Kumble R. Subbaswamy
Chancellor
University of Massachusetts Amherst

11/14/16

Date

For United States Department of Health and Human Services



Susan M. Pezzullo Rhodes
Regional Manager, New England Region
Office for Civil Rights

11/16/16

Date