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 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 Mississippi ("UM"), which is a covered entity, as defined at 45 C.F.R. § 160.103, and therefore required to comply with the HIPAA Rules, on behalf of the University of Mississippi Medical Center ("UMMC"), which is a designated health care component of UM.[1] UM is Mississippi's sole public academic health science center, with education and research functions in addition to providing patient care in four specialized hospitals and clinics on the Jackson campus and at clinics throughout Jackson and the State.

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

2. Factual Background and Covered Conduct

   On March 21, 2013, the HHS Office for Civil Rights ("OCR") received notification from UMMC regarding a breach of unsecured electronic protected health information ("ePHI") affecting 500 or more individuals at UMMC's University Hospital. On October 25, 2013, HHS notified UMMC of its investigation regarding UM's compliance with the Privacy, Security, and Breach Notification Rules.

[1] The University of Mississippi ("UM") is a covered entity, as defined at 45 C.F.R. § 160.103, and a hybrid entity, as defined at 45 C.F.R. § 164.103, whose operations include both covered and non-covered functions and which has designated health care components, including the University of Mississippi Medical Center ("UMMC"), in accordance with 45 C.F.R. § 164.105(a)(2)(iii)(D). Other than certain oversight, compliance and enforcement obligations, as set forth at 45 C.F.R. §§ 164.105, 164.314, and 164.504, which apply to UM, the remaining provisions of the HIPAA Rules apply only to the health care components of UM, including UMMC. *See* 45 C.F.R. § 164.105(a)(1).

OCR's investigation indicated UM[2] had implemented policies and procedures pursuant to the HIPAA Rules; however, OCR's investigation indicated that the following conduct occurred ("Covered Conduct"):

A. From the compliance date of the Security Rule, April 20, 2005, until present, UM failed to implement policies and procedures to prevent, detect, contain, and correct security violations, including conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI it holds, and implementing 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. From January 19, 2013, until March 1, 2014, UM failed to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users (*See* 45 C.F.R. §164.310(c));

C. From the compliance date of the Security Rule, April 20, 2005, to March 14, 2013, UM failed to assign a unique user name and/or number for identifying and tracking user identity in information systems containing ePHI including, for example, allowing workforce members to access ePHI on a shared department network drive through a generic account, preventing UMMC from tracking which specific users were accessing ePHI (*See* 45 C.F.R. § 164.312 (a)(2)(i)); and

D. UM, following the discovery of this breach of unsecured ePHI, provided notification on UMMC's website and in local media outlets, but failed to notify each individual whose unsecured ePHI was reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach (*See* 45 C.F.R. §164.404).

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

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

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve OCR Transaction No. 13-157615, and any 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.

[2] Hereinafter in this Agreement and Corrective Action Plan ("CAP"), any reference to UM shall include UMMC as a covered health care component of UM.

II. Terms and Conditions

6. Payment. HHS has agreed to accept, and UM has agreed to pay HHS, the amount of $2,750,000 ("Resolution Amount"). UM agrees to pay the Resolution Amount on the Effective Date of this Agreement as defined in paragraph II.14 by automated clearinghouse transaction pursuant to written instructions to be provided by HHS.

7. Corrective Action Plan. UM 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 UM breaches the CAP, and fails to cure the breach as set forth in the CAP, then UM 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 UM's performance of its obligations under this Agreement, HHS releases UM from any actions it has or may have against UM under the HIPAA Rules arising out of or related to the Covered Conduct specified in paragraph I.2. of this Agreement. HHS does not release UM 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 Party. UM 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. UM 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, 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 UM 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 must 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, UM agrees that the time between the Effective Date of this Agreement and the date the Agreement may be terminated by reason of UM'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. UM waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct specified 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 UM represent and warrant that they are authorized by The University of Mississippi 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 The University of Mississippi

/s/ July 7, 2016
LouAnn Woodward, MD Date
Vice Chancellor
University of Mississippi Medical Center

For the United States Department of Health and Human Services

/s/ July 7, 2016
Michael Leoz Date
Regional Manager, Pacific Region
Office for Civil Rights

Appendix A

CORRECTIVE ACTION PLAN

BETWEEN THE

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

THE UNIVERSITY OF MISSISSIPPI

I. Preamble

The University of Mississippi (hereinafter referred to as "UM"), on behalf of the University of Mississippi Medical Center (hereinafter referred to as "UMMC"),[3] 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, UM is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Agreement as Appendix A. UM enters into this CAP as part of the consideration for the release set forth in paragraph 8 of the Agreement.

II. Contact Persons and Submissions

A. Contact Persons

UM 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:

Carol Denton, Chief Integrity and Compliance Officer
University of Mississippi Medical Center
2500 North State Street
Jackson, MS 39216

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

Evelyn Zeller, Supervisor, OCR Pacific Region
U.S. Department of Health & Human Services, Office for Civil Rights
701 Fifth Avenue, Suite 1600, MS-11
Seattle, WA 98104

[3] Hereinafter in this Corrective Action Plan ("CAP"), any reference to UM shall include UMMC as a covered health care component of UM.

UM 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 II.14 of the Agreement ("Effective Date"). The period for compliance ("Compliance Term") with the obligations assumed by UM under this CAP shall begin on the Effective Date of this CAP and end three (3) years from the date HHS approves the Security Management Process required by section V.B., unless HHS has notified UM under Section VIII hereof of its determination that UM 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 UM that it has determined that the breach has been cured. After the Compliance Term ends, UM 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.

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 that is not one of the aforementioned days.

V. Corrective Action Obligations

UM agrees to the following:

A. Monitoring.

1. Designation of Internal Monitor. Within sixty (60) days of the Effective Date, UM shall designate a qualified workforce member of UM to be an Internal Monitor and to review UM's compliance with this CAP. The Internal Monitor must certify in writing that he/she has expertise in compliance with the HIPAA Rules and is able to perform the tasks described below in a professionally independent fashion, taking into account his/her employment or professional relationship with UM and any other business relationships or engagements that

may exist. Within the above-referenced time period, UM shall submit the name and qualifications of the designated individual to HHS for HHS's approval. Upon receiving such approval, UM shall formally designate the workforce member as Internal Monitor for the reviews specified below.

2. Monitor Plan. Within thirty (30) days of being approved for service by HHS, the Internal Monitor shall submit to HHS and UM a written plan, describing with adequate detail, the Internal Monitor's plan for fulfilling the duties set forth in this subsection (Monitor's Plan). Those duties include reviewing and providing technical assistance to UM, as necessary and appropriate, on all policies and procedures and training materials drafted or revised by UM, or otherwise prepared for UM, to satisfy any requirement of this CAP. Within thirty (30) days of its receipt of the Monitor's Plan, HHS may submit comments and recommended changes to the Monitor's Plan. The Internal Monitor shall make such changes to the Plan as HHS may reasonably have requested. The Internal Monitor shall review the Plan at least annually and shall provide HHS and UM with a copy of any revisions to the Plan within ten (10) days of the Internal Monitor's making such revisions. HHS shall have a reasonable opportunity to comment and make recommendations regarding any revisions or modifications at any time while the CAP is in effect. The Internal Monitor shall make such changes to the revisions as HHS may reasonably request.

3. Retention of Records. The Internal Monitor and UM shall retain and make available to HHS, upon request, all work papers, supporting documentation, correspondence, and draft reports (those exchanged between the Internal Monitor and UM) related to the reviews.

4. Description of Monitor Reviews. The Monitor reviews shall address and analyze UM's compliance with this CAP. The Internal Monitor will conduct quarterly progress meetings with UM's Security Official, interview workforce members as needed and follow-up on reports of possible security violations.

5. Monitor Review Reports and Response. The Internal Monitor shall prepare a quarterly report based on the reviews and other activities it has performed related to the Monitor's Plan and provide such report to HHS and UM. UM shall prepare a response to the report and provide such response to HHS and the Internal Monitor. The Internal Monitor shall immediately report any significant violations of the CAP to HHS and UM, and UM shall prepare a response, including a plan(s) of correction, and provide such response to HHS and the Internal Monitor.

6. Internal Monitor Removal/Termination. If UM intends to terminate or remove the designation of any Internal Monitor during the Compliance Term of this CAP, UM must submit a notice explaining its reasons to HHS prior to the termination or removal of designation, unless exigent circumstances require immediate termination or removal of designation. UM must designate a new Internal Monitor in accordance with this CAP within sixty (60) days of terminating or removing the designation of the previous Internal Monitor. In the

event HHS has reason to believe that an Internal Monitor does not possess the expertise, independence, or objectivity required by this CAP, or has failed to carry out his/her responsibilities as set forth in this CAP, HHS may, at its sole discretion, require UM to designate a new Internal Monitor in accordance with this CAP. Prior to requiring UM to designate a new Internal Monitor, HHS shall notify UM of its intent to do so and provide a written explanation of why HHS believes such a step is necessary.

7. Validation Review. In the event HHS has reason to believe that (a) the Monitor reviews or reports fail to conform to the requirements of this CAP; or (b) the Monitor report results are inaccurate, HHS may, at its sole discretion, conduct its own review to determine whether the Monitor reviews or reports complied with the requirements of the CAP and/or are inaccurate ("Validation Review").

Prior to initiating a Validation Review, HHS shall notify UM of its intent to do so and provide a written explanation of why HHS believes such a review is necessary. To resolve any concerns raised by HHS, UM may request a meeting with HHS to discuss the results of any Monitor Review submissions or findings; present any additional or relevant information to clarify the results of the Monitor Review to correct the inaccuracy of the Monitor Review; and/or propose alternatives to the proposed Validation Review. UM shall provide any additional information as may be requested by HHS under this Section in an expedited manner. HHS will attempt in good faith to resolve any Monitor Review concerns with UM prior to conducting a Validation Review. However, the final determination as to whether or not to proceed with a Validation Review shall be made at the sole discretion of HHS.

8. The use of the Internal Monitor does not affect HHS's authority to investigate complaints or conduct compliance reviews itself, or UM's responsibilities under 45 C.F.R. Part 160, Subpart C.

B. Security Management Process.

1. UM shall draft an enterprise-wide risk analysis and corresponding risk management plan[4] that includes security measures to reduce the risks and vulnerabilities to the electronic protected health information (ePHI) maintained by UM to a reasonable and appropriate level. The risk analysis and corresponding risk management plan shall accurately reflect the enterprise-wide environment and operations of UM that exist at the time the risk analysis and risk management plan are submitted to HHS, including evaluating and addressing any weaknesses in the UM organizational structure (including staff qualifications and authority) responsible for overseeing UM's compliance with the HIPAA Rules.

2. UM shall provide the updated risk analysis and risk management plan to the Internal Monitor for review and approval within ninety (90) days of HHS's approval of the Monitor Plan specified in Section V.A.2.

[4] The risk analysis and risk management shall encompass all covered health care components.

3. Within fifteen (15) days of receiving approval from the Internal Monitor, UM shall submit the updated risk analysis and risk management plan to HHS for review and approval. Upon receiving notice from HHS specifying any required changes, UM shall make the required changes and provide a revised risk analysis and risk management plan to HHS and the Internal Monitor within sixty (60) days of receiving any notice from HHS requiring any changes.

4. UM shall initiate implementation of security risk management activities under the risk management plan no later than thirty (30) days following receipt of HHS's approval.

C. Security Rule Policies and Procedures

1. UM shall update its *Information Security Policy*, and any necessary additional policies or procedures, as required to comply with 45 C.F.R. Parts 160 and 164, Subpart C (The Security Rule) and specifically 45 C.F.R. § 164.316, which apply to all covered health care components.

2. UM shall provide the updated *Information Security Policy*, and any additional policies and procedures, to the Internal Monitor for review and approval within ninety (90) days of HHS's approval of UM's risk analysis and risk management plan required by Section V.B.

3. Within fifteen (15) days of receiving approval from the Internal Monitor, UM shall submit the *Information Security Policy*, and any additional policies and procedures, to HHS for review and approval. Upon receiving notice from HHS specifying any required changes, UM shall make the required changes and provide a revised *Information Security Policy*, and any additional policies and procedures, to HHS and the Internal Monitor within thirty (30) days.

4. UM shall officially adopt and implement such policies and procedures within thirty (30) days of receipt of HHS's approval.

D. Breach Notification

1. UM shall revise its current *Breach of Unsecured Protected Health Information Notification* policy (revision date September 2013) to state, in "Section 3.0 Standards," that UM shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by UM to have been, accessed, acquired, used, or disclosed as a result of a breach as required by 45 C.F.R. § 164.404.

2. UM shall provide the revised *Breach of Unsecured Protected Health Information Notification* policy to the Internal Monitor for review and approval within ninety (90) days of HHS's approval of UM's risk analysis and risk management plan required by Section V.B.

3. Within fifteen (15) days of receiving approval from the Internal Monitor, UM shall submit the *Breach of Unsecured Protected Health Information Notification* policy to HHS for review and approval. Upon receiving notice from HHS specifying any required changes, UM shall make the required changes and provide a revised *Breach of Unsecured Protected Health Information Notification* policy to HHS and the Internal Monitor within thirty (30) days.

4. UM shall officially adopt and implement the revised *Breach of Unsecured Protected Health Information Notification* policy within thirty (30) days of receipt of HHS's approval.

E. Unique User Identification

1. UM shall provide the Internal Monitor with a plan to require a unique name and/or number identifying and tracking users of all information systems that contain ePHI, including departmental shared network drives. UM shall provide the plan to require a unique user name and/or number to the Internal Monitor for review and approval within ninety (90) days of HHS's approval of UM's risk analysis and risk management plan required by Section V.B.

2. Within fifteen (15) days of receiving approval from the Internal Monitor, UM shall provide the plan to HHS for review and approval. Upon receiving notice from HHS specifying any required changes, UM shall make the required changes and provide the revised plan to HHS and the Internal Monitor within thirty (30) days.

3. Upon receiving approval of its plan from HHS, UM shall begin implementing the plan within thirty (30) days of receipt of HHS's approval.

4. UM shall provide the Internal Monitor with quarterly updates of the progress of the plan including documentation.

F. Security Awareness and Training.

1. UM shall provide the Internal Monitor with its security awareness and training program materials for all workforce members (including management) of its covered health care components who have access to ePHI in accordance with 45 C.F.R.§164.308(a)(5), to include specific training related to its new policies and procedures under Sections V.C., V.D., and V.E., within sixty (60) days of HHS's approval of the last of UM's policies and procedures in Sections V.C., V.D., and V.E. to receive HHS's approval.

2. Within fifteen (15) days of receiving approval from the Internal Monitor, UM shall provide the security awareness and training materials to HHS for review and approval. Upon receiving notice from HHS specifying any required changes, UM shall make the required changes and provide revised security awareness and training materials to HHS and the Internal Monitor within thirty (30) days.

3. Upon receiving approval of its security awareness and training materials from HHS, UM shall initiate security awareness and training for all workforce members of its covered health care components with access to ePHI within thirty (30) days of receipt of HHS's approval. Any new members of UM's covered health care components' workforce that are hired after the initial training period described in this paragraph shall be trained within 30 days of their beginning as a member of the workforce.

4. UM shall provide the Internal Monitor with quarterly updates of the progress of the security awareness and training program including documentation of completed training and a schedule for any pending training.

5. UM shall review the approved security awareness and training materials annually, and, where appropriate, update the security awareness and training to reflect changes in Federal law or HHS guidance, any changes to its security policies and procedures, any issues discovered during audits or reviews, and any other relevant developments.

G. Reportable Events.

1. UM shall, upon receiving information that a workforce member of a covered health care component may have failed to comply with its privacy and security policies and procedures or otherwise that there may have been a violation of the HIPAA Privacy, Security or Breach Notification Rules, promptly investigate the matter. If UM determines, after review and investigation, that a member of the workforce of a covered health care component has failed to comply with its privacy and security policies and procedures or that there has otherwise been a violation of the HIPAA Privacy, Security or Breach Notification Rules, UM shall notify the Internal Monitor and HHS in writing within thirty (30) days of its determination. 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 UM's privacy and security policies and procedures or HIPAA Privacy, Security or Breach Notification Rules implicated; and

b. A description of the actions taken and any further steps UM 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 and security policies and procedures or otherwise violated the HIPAA Privacy, Security or Breach Notification Rules.

c. If no Reportable Events have occurred during the Compliance Term, UM shall so inform the Internal Monitor and HHS in writing thirty (30) days prior to the conclusion of the Compliance Term.

VI. Implementation Report and Annual Reports

A. Implementation Report. Within ninety (90) days after the receipt of HHS's approval of the Security Awareness and Training materials required by Section V.F., UM shall submit a written report to HHS and the Internal Monitor summarizing the status of its implementation of the requirements of this CAP. This report, known as the "Implementation Report," shall include:

1. An attestation signed by an officer of UM attesting that the security risk management activities under the risk management plan required by Section V.B. are being implemented;

2. An attestation signed by an officer of UM attesting that the policies and procedures required by Sections V.C., V.D., and V.E. are being implemented and have been distributed to all appropriate workforce members of its covered health care components;

3. The formal designation of the Internal Monitor, a summary description of all employment and professional engagements between UM and the Internal Monitor, including, but not limited to, any outside financial audits, compliance program engagements, or reimbursement consulting, and the proposed start and completion dates of the first Monitor Review;

4. A copy of the certification from the Internal Monitor regarding his/her expertise in compliance with the HIPAA Rules and ability to perform the tasks of the Internal Monitor in the CAP in a professionally independent fashion as required by Section V.A.1;

5. An attestation signed by an officer of UM listing all UM facilities and locations covered by this Resolution Agreement and Corrective Action Plan, including mailing addresses, the corresponding name under which each facility is doing business, the corresponding phone numbers and fax numbers, and attesting that each such facility has complied with the obligations of this CAP; and

6. An attestation signed by an officer of UM stating that he or she has reviewed the Implementation Report, has made a reasonable inquiry regarding its contents 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." UM also shall submit to HHS and the Internal Monitor Annual Reports with respect to the status of and findings regarding UM's compliance with this CAP for each of the Reporting Periods. UM shall submit each Annual Report to HHS no later than sixty (60) days after the end of each corresponding Reporting Period. The Annual Report shall include:

1. A summary of the security risk management measures (defined in Section V.B.) taken during the Reporting Period;

2. A status report of the implementation of the policies and procedures and workforce training as required by Sections V.C. - V.F. during the Reporting Period, including documentation of completed training, a schedule of pending training, and copies of the training materials, if different than those approved by HHS in Section V.F.2;

3. A summary description of all employment and professional engagements between UM and the Internal Monitor, including, but not limited to, any outside financial audits, compliance program engagements, or reimbursement consulting, if different from what was submitted as part of the Implementation Report;

4. A summary of Reportable Events (defined in Section V.G.) identified during the Reporting Period and the status of any corrective and preventative action relating to all such Reportable Events;

5. An attestation signed by an officer of UM 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

UM 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

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

A. Timely Written Requests for Extensions. UM 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. The Parties agree that a breach of this CAP by UM constitutes a breach of the Agreement. Upon a determination by HHS that UM has breached this CAP, HHS may notify UM of (1) UM's breach; and (2) HHS's 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 at paragraph I.2. of the Agreement and any other conduct that constitutes a violation of the HIPAA Rules ("Notice of Breach and Intent to Impose CMP").

C. UM's Response. UM shall have thirty (30) days from the date of receipt of the Notice of Breach and Intent to Impose CMP to demonstrate to HHS's satisfaction that:

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

2. the alleged breach has been cured; or

3. the alleged breach cannot be cured within the thirty (30) day period, but that: (a) UM has begun to take action to cure the breach; (b) UM is pursuing such action with due diligence; and (c) UM 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, UM fails to meet the requirements of section VIII.C of this CAP to HHS's satisfaction, HHS may proceed with the imposition of a CMP against UM pursuant to 45 C.F.R. Part 160 for any violations of the HIPAA Rules related to the Covered Conduct set forth at paragraph I.2. A.-D. of the Agreement and for any other act or failure to act that constitutes a violation of the HIPAA Rules. HHS shall notify UM in writing of its determination to proceed with the imposition of a CMP.

For The University of Mississippi

/s/ July 7, 2016
LouAnn Woodward, MD Date
Vice Chancellor
University of Mississippi Medical Center

For the United States Department of Health and Human Services

/s/ July 7, 2016
Michael Leoz Date
Regional Manager, Pacific Region
Office for Civil Rights