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 that govern 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. Oregon Health & Science University ("OHSU"), which meets the definition of a "covered entity" under 45 C.F.R. § 160.103, is required to comply with the HIPAA Rules.

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

2. Factual Background and Covered Conduct. On March 23, 2013, HHS received notification from OHSU regarding a breach of its unsecured electronic protected health information ("ePHI") resulting from a stolen laptop computer. On July 28, 2013, HHS received notification from OHSU regarding a breach of its ePHI resulting from storing ePHI at an internet-based service provider without a business associate agreement. On May I, 2013, and on November 8, 2013, HHS notified OHSU of its investigations of these breach incidents, respectively, regarding OHSU's compliance with the HIPAA Rules.

HHS's investigations indicated that OHSU had implemented policies and procedures pursuant to the HIPAA Rules; however, HHS's investigations indicated the following conduct occurred ("Covered Conduct").

A. From January 5, 2011, until July 3, 2013, OHSU disclosed the ePHI of 3,044 individuals in violation of the Privacy Rule (*See* 45 C.F.R. §§160.103 and 164.502 (a)) when workforce members disclosed the ePHI to a third party internet-based service provider without obtaining a business associate agreement or other satisfactory assurance that the internet-based service provider would safeguard the ePHI;

B. From January 5, 2011, until July 3, 2013, OHSU failed to obtain a business associate agreement from an internet-based service provider that was storing ePHI on its behalf as a business associate as required by 45 C.F.R. § 164.308(b);

C. From January 5, 2011, until July 3, 2013, OHSU failed to implement policies and procedures to prevent, detect, contain, and correct security violations. (*See* 45 C.F.R. § 164.308(a)(1)(i);

D. From July 12, 2010, to present, OHSU failed to implement a mechanism to encrypt and decrypt ePHI or an equivalent alternative measure for all ePHI maintained in OHSU's enterprise. (*See* 45 C.F.R. §§ 164.312(a)(2)(iv) and 164.306(d)(3)); and

E. From May 29, 2013, until July 3, 2013, OHSU failed to implement policies and procedures to address security incidents. (*See* 45 C.F.R. § 164.308(a)(6)(i)).

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

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

5. Intention of Parties to Effect Resolution. This Agreement is intended to resolve HHS Transaction Numbers 13-157605 and 13-163586 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.

II. Terms and Conditions

6. Payment. HHS has agreed to accept, and OHSU has agreed to pay HHS, the amount of $2,700,000 ("Resolution Amount"). OHSU 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. OHSU 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 OHSU breaches the CAP, and fails to cure the breach as set forth in the CAP, then OHSU 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 OHSU's performance of its obligations under this Agreement, HHS releases OHSU from any actions it may have against OHSU 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 OHSU 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. OHSU 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. OHSU 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 OHSU and its successors, heirs, transferees, and assigns.

11. Costs. Each Party to this Agreement shall bear its own legal and other costs incurred in connection with this matter, including the preparation and performance of this Agreement.

12. No Additional Releases. This Agreement is intended to be for the benefit of the Parties only, and by this instrument the Parties do not release any claims against any other person or entity.

13. Effect of Agreement. This Agreement constitutes the complete agreement between the Parties. All material representations, understandings, and promises of the Parties are contained in this Agreement. Any modifications to this Agreement shall be set forth in writing and signed by all Parties.

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

15. Tolling of Statute of Limitations. Pursuant to 42 U.S.C. § 1320a-7a(c)(1), a civil money penalty 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, OHSU agrees that the time between the Effective Date of this Agreement and the date the Agreement may be terminated by reason of OHSU'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. OHSU waives and will not plead any statute of limitations, laches, or similar defenses to any administrative action relating to the Covered Conduct identified in paragraph 1.2 that is filed by HHS within the time period set forth above, except to the extent that such defenses would have been available had an administrative action been filed on the Effective Date of this Agreement.

16. Disclosure. HHS places no restriction on the publication of the Agreement. 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 OHSU represent and warrant that they are authorized by OHSU 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 Oregon Health & Science University

/s/ _____

Lawrence Furnstahl
Executive Vice President & Chief Financial Officer Oregon Health & Science University

Date

For United States Department of Health and Human Services

/s/ _____

Michael Leoz
Regional Manager, Pacific Region Office for Civil Rights

Date

Appendix A

CORRECTIVE ACTION PLAN

BETWEEN THE

UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND THE

OREGON HEALTH & SCIENCE UNIVERSITY

I. Preamble

The Oregon Health & Science University (hereinafter known as "OHSU") 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, OHSU is entering into a Resolution Agreement ("Agreement") with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. OHSU 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

OHSU 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:

Randy Gainer, Partner
Baker & Hostetler, LLP
999 Third Avenue, Suite 3600
Seattle, WA 98104
Voice: (206) 332-1381
Fax: (206) 624-7317

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

Evelyn Zeller, Supervisory Equal Opportunity Specialist, OCR Pacific Region
701 Fifth Avenue, Suite 1600, MS-11
Seattle, WA 98104
Voice: (206) 615-2290
Fax: (206) 615-2297

OHSU 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 OHSU under this CAP shall begin on the Effective Date of this CAP and end three (3) years from the Effective Date unless a) HHS has notified OHSU under section VIII.B. hereof of its determination that OHSU breached this CAP, or b) HHS has agreed to OHSU's request for an extension of a due date under section VIII.A. hereof to perform any act required by this CAP with the result that the new due date would fall outside of the Compliance Term. In the event of such a notification by HHS under section VIII.B. hereof, the Compliance Term shall not end until HHS notifies OHSU that it has determined that the breach has been cured. In the event HHS has agreed to extend a due date under section VIII.A. hereof as described previously in this paragraph, the Compliance Term of this CAP shall not end until HHS notifies OHSU that it has approved OHSU's completion of the required act for which an extension was granted. After the Compliance Term ends, OHSU 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 which is not one of the aforementioned days.

V. Corrective Action Obligations

OHSU agrees to the following:

A. Security Management Process.

1. OHSU shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information ("ePHI") held at OHSU, to include all OHSU facilities located in and outside of Portland, Oregon, and all systems, networks, and devices that create, receive, maintain, or transmit ePHI.

2. OHSU shall develop a comprehensive risk management plan that explains OHSU's strategy for implementing security measures sufficient to reduce the risks and vulnerabilities identified in the risk analysis to a reasonable and appropriate level based on OHSU's circumstances. OHSU's risk management plan shall include a comprehensive, enterprise-wide plan to implement effective oversight of OHSU workforce members to ensure their adherence to HIPAA Rules and OHSU's internal privacy and security policies and procedures. For all planned remediation actions, OHSU shall provide specific timelines for their expected completion and identify the compensating controls that will be in place in the interim to safeguard OHSU's ePHI.

3. Within three hundred ten (310) days of the Effective Date, OHSU shall provide its risk analysis and risk management plan (including implementation dates for such measures and interim compensating controls) to HHS for review and approval. Upon receiving any recommended changes to the risk analysis and risk management plan from HHS, OHSU shall have ninety (90) days to revise the risk analysis and risk management plan and provide the revisions to HHS for review and approval.

B. Encryption Status Update Requirements

Within three hundred ten (310) days of the Effective Date, at two years following the Effective Date, and at each subsequent year following the Effective Date during the term of the CAP, OHSU shall provide an update to HHS regarding its encryption status, which shall include:

1. The status, including supporting evidence, of OHSU's implementation of a Mobile Device Management (MDM) solution that will ensure all OHSU-owned and personally-owned mobile devices (tablets, smart phones, and other mobile devices) that access ePHI on OHSU's secure network are encrypted, except for any mobile devices for which OHSU has granted exceptions to the encryption requirement. If OHSU has granted exceptions for the encryption requirement to any mobile devices, it will provide evidence of reasonable compensating controls that have been implemented to protect the ePHI on such devices. OHSU shall complete initial deployment of an MDM solution within three hundred ten (310) days of the Effective Date.

2. The status, including supporting evidence, of OHSU's implementation of a solution to enforce encryption of ePHI on OHSU-owned and personally-owned devices (laptops, desktops, and medical equipment) connecting to OHSU's secure wired and wireless networks except for any devices for which OHSU has granted exceptions to the encryption requirement. If OHSU has granted an exception for the encryption requirement to any devices, it will provide evidence of reasonable compensating controls that

have been implemented to protect the ePHI on such devices. OHSU will periodically test the effectiveness of its implemented solution to enforce encryption on OHSU-owned and personally-owned devices (laptops, desktops, and medical equipment) connecting to OHSU's secure wired network except for any devices for which OHSU has granted exceptions to the encryption requirement. OHSU shall complete initial deployment of a solution to enforce encryption of ePHI on devices connecting to OHSU's secure wireless network within two years of the Effective Date.

3. Implementation of policies that prohibit the transfer of data containing ePHI from OHSU-owned and personally-owned devices to unencrypted removable storage devices (USB drives and portable hard drives) and implementation of a technical solution that enforces the policies prohibiting transfers of this type when attached to the OHSU secure network, except for any removable storage devices for which OHSU has granted exceptions to the encryption requirement. If OHSU has granted an exception for the encryption requirement to any removable storage devices, it will provide evidence of reasonable compensating controls that have been implemented to protect the ePHI on such devices. OHSU shall complete initial deployment of a solution to enforce encryption for removable storage devices within three years of the Effective Date. OHSU shall periodically test the effectiveness of its implemented solution to enforce encryption on removable storage devices.

C. Security Awareness and Training.

1. OHSU shall send a communication to all members of the OHSU community describing its commitment to enterprise encryption by August 15, 2016.

2. OHSU shall provide HHS with its training materials relating to security awareness established to reduce the risks and vulnerabilities to ePHI as identified in its security management process in section V.A. OHSU's training materials shall also include privacy and security awareness related to a) use of internet-based information storage services; 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 protected health information (PHI) and/or ePHI; c) regarding managers, effective oversight of workforce members' uses and disclosures of PHI, including ePHI, to ensure the workforce members' compliance with the Privacy and Security Rules and OHSU's internal policies and procedures; d) security incident reporting; and e) password management. OHSU shall provide the training materials to HHS for review and approval within ninety (90) days of the date HHS has approved OHSU's risk analysis and risk management plan in section V.A.

3. Upon receiving notice from HHS specifying any required changes, OHSU shall make the required changes and provide revised privacy and security awareness training materials to HHS within sixty (60) days.

4. Upon receiving approval from HHS, OHSU shall provide documentation that a) all workforce members with access to PHI and/or ePHI have received such privacy and security awareness training within one hundred twenty (120) days; b) that these workforce members will continue to receive such training on an on-going basis; and c) that each new OHSU workforce member with access to PHI and/or ePHI will receive such security awareness training within fifteen (15) days of beginning work at OHSU.

5. OHSU shall review the security awareness 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. The one-year period beginning on the Effective Date and each following one-year period shall be referred to as "the Reporting Periods." During each Reporting Period under this CAP, OHSU shall, upon receiving information that a workforce member may have failed to comply with its HIPAA Rules policies and procedures, promptly investigate the matter. If OHSU, after review and investigation, determines that a member of the workforce has failed to comply with its HIPAA Rules policies and procedures, OHSU shall notify HHS in writing within 30 days. Such violations shall be known as "Reportable Events." The report to HHS shall include the following:

2. A complete description of the event, including the relevant facts, the persons involved, and the provision(s) of OHSU's HIPAA Rules policies and procedures implicated; and

3. A description of the actions taken and any further steps OHSU 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 HIPAA Rules policies and procedures.

4. If no Reportable Events have occurred within a Reporting Period, OHSU shall so inform HHS in its Annual Report for that Reporting Period in accordance with section VI. of this CAP.

VI. Annual Reports

OHSU shall submit to HHS Annual Reports with respect to the status of and findings regarding

OHSU's compliance with this CAP for each of the Reporting Periods. OHSU 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:

A. A summary of the security management measures (defined in section V.A.) taken during the Reporting Period;

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

C. An attestation signed by an officer of OHSU 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

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

VIII. Breach Provisions

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

A. Timely Written Requests for Extensions. OHSU 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 OHSU constitutes a breach of the Agreement. Upon a determination by HHS that OHSU has breached this CAP, HHS may notify OHSU of (1) OHSU's breach; and (2) HHS' intent to impose a civil money penalty ("CMP") pursuant to 45 C.F.R. Part 160, or other remedies for the Covered Conduct set forth in paragraph 1.2 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. OHSU's Response. OHSU 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. OHSU 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 thirty (30) day period, but that (a) OHSU has begun to take action to cure the breach; (b) OHSU is

pursuing such action with due diligence; and (c) OHSU 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, OHSU 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 OHSU pursuant to 45 C.F.R. Part 160 for any violations of HIPAA Rules related to the Covered Conduct set forth in paragraph 1.2 of the Agreement and for any other act or failure to act that constitutes a violation of the HIPAA Rules. HHS shall notify OHSU in writing of its determination to proceed with the imposition of a CMP.

For Oregon Health & Science University

/s/ _____

Lawrence Furnstahl
Executive Vice President & Chief Financial Officer Oregon Health & Science University

Date

For United States Department of Health and Human Services

/s/ _____

Michael Leoz
Regional Manager, Pacific Region Office for Civil Rights

Date