DEPARTMENT OF HEALTH & HUMAN SERVICES
Voice - (206) 615-2290, (800) 362-1710
TDD - (206) 615-2296, (800) 537-7697
(FAX) - (206) 615-2297
http://www.hhs.gov/ocr/

OFFICE OF THE SECRETARY
Office for Civil Rights, Region X
2201 Sixth Avenue, Mail Stop RX-11
Seattle, WA 98121-1831

Date: APR 05 2013

Arthur C. Vailas, President
Idaho State University
Administration Building
921 South 8th Avenue, STOP 8310
Pocatello, ID 83209-8310

OCR Transaction Number: 11-130876

Dear Mr. Vailas:

This letter is to inform you that the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) has completed its investigation of Idaho State University (ISU), which was conducted pursuant to OCR's authority under the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules). To resolve the issues raised in the investigation, OCR is offering the enclosed Resolution Agreement and Corrective Action Plan. If ISU agrees to the terms of the Resolution Agreement and Corrective Action Plan, it has until Monday, May 20, 2013 to sign and return the documents. ISU must remit payment within ten days of signing and OCR will provide specific instructions on the transfer of funds. If OCR does not have the signed documents and payment within the specified timeframe, the terms of the Resolution Agreement will no longer be available. OCR will proceed to formal enforcement of this matter.

Under the Freedom of Information Act, we may be required to release this letter and other information about this case upon request by the public. In the event OCR receives such a request, we will make every effort, as permitted by law, to protect information that identifies individuals or that, if released, could constitute a clearly unwarranted invasion of personal privacy.

If you have any questions, please contact Sunil Abraham, Assistant Regional Counsel, at (206) 615-2281 or Sunil.Abraham@hhs.gov.

Sincerely,

L-Yuu Connor

Linda Yuu Connor
Regional Manager

Enclosure: Resolution Agreement and Corrective Action Plan

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 Idaho State University (ISU).

2. Authority of HHS. HHS 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") and 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"). HHS has the authority to conduct the investigations of complaints alleging violations of the Privacy and Security Rules by covered entities, and covered entities must cooperate with HHS' investigation. 45 C.F.R. § 160.306(c) and §160.310(b).

3. Factual Background and Covered Conduct. On August 9, 2011, HHS received notification from ISU regarding a breach of its unsecured electronic protected health information (ePHI). On November 22, 2011, HHS notified ISU of its investigation regarding ISU's compliance with the Privacy, Security, and Breach Notification Rules. HHS' investigation indicated that the following conduct occurred ("Covered Conduct").

i. ISU did not conduct an analysis of the risk to the confidentiality of ePHI as part of its security management process from April 1, 2007 until November 26, 2012;

ii. ISU did not adequately implement security measures sufficient to reduce the risks and vulnerabilities to a reasonable and appropriate level from April 1, 2007 until November 26, 2012; and

iii. ISU did not adequately implement procedures to regularly review records of information system activity to determine if any ePHI was used or disclosed in an inappropriate manner from April 1, 2007 until June 6, 2012.

4. No Admission. This Agreement is not an admission of liability by ISU.

5. No Concession. This Agreement is not a concession by HHS that ISU is not in violation of either the Privacy Rule or the Security Rule and that ISU is not liable for civil money penalties.

6. Intention of Parties to Effect Resolution. This Agreement is intended to resolve HHS Transaction Number: 11-130876, and any violations of the HIPAA Privacy and Security Rules for the Covered Conduct specified in paragraph 3 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

7. Payment. ISU agrees to pay HHS the amount of $400,000 (Resolution Amount). ISU agrees to pay the Resolution Amount by electronic funds transfer pursuant to written instructions to be provided by HHS. ISU agrees to make this payment within 10 days of the Effective Date.

8. Corrective Action Plan. ISU 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 ISU breaches the CAP, and fails to cure the breach as set forth in the CAP, then ISU will be in breach of this Agreement and HHS will not be subject to the Release set forth in paragraph 9 of this Agreement.

9. Release by HHS. In consideration and conditioned upon ISU's performance of its obligations under this Agreement, HHS releases ISU from any actions it may have against ISU under the Privacy and Security Rules for the covered conduct identified in paragraph 3. HHS does not release ISU 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.

10. Agreement by Released Parties. ISU 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. ISU 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.

11. Binding on Successors. This Agreement is binding on ISU and its successors, heirs, transferees, and assigns.

12. 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.

13. 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.

14. 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.

15. 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 HHS (Effective Date).

16. 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, ISU agrees that the time between the Effective Date of this Resolution Agreement (as set forth in paragraph 15) and the date the Resolution Agreement may be terminated by reason of ISU'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. ISU waives and will not plead any statute of limitations, laches, or similar defenses to any action for the covered conduct identified in paragraph 3 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 action been filed on the Effective Date of this Resolution Agreement.

17. 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.

18. 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.

19. Authorizations. The individual(s) signing this Agreement on behalf of ISU represent and warrant that they are authorized by ISU 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 Idaho State University

_____ _____

Arthur C. Vailas, President
Idaho State University

Date

For United States Department of Health and Human Services

_____ _____

Linda Yuu Connor
Regional Manager, Region X
Office for Civil Rights

Date

Appendix A

CORRECTIVE ACTION PLAN

BETWEEN THE

UNITED STATES DEPARTMENT OF HEALTH AND HUMAN SERVICES

AND

IDAHO STATE UNIVERSITY

I. Preamble

Idaho State University (ISU) 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, ISU is entering into a Resolution Agreement with HHS, and this CAP is incorporated by reference into the Resolution Agreement as Appendix A. ISU enters into this CAP as consideration for the release set forth in paragraph 9 of the Resolution Agreement.

II. Contact Persons and Submissions

A. Contact Persons

ISU 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:

Arthur C. Vailas, President
Idaho State University
Administration Building
921 South 8th Avenue, STOP 8310
Pocatello, ID 83209-8310
Voice: (208) 282-3440
Fax: (208) 282-4821

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

Linda Yuu Connor, Regional Manager, OCR Region X
2201 Sixth Avenue, Mail Stop: RX-11
Seattle, WA 98121-1831
Voice: (206) 615-2290
Fax: (206) 615-2297

ISU 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. Term of CAP

The period of compliance obligations assumed by ISU under this CAP shall begin on the Effective Date of this CAP and end two years from the Effective Date, except that after this period ISU shall be obligated to (a) submit the Annual Report for the final Reporting Period, as set forth in section VI. and (b) comply with the document retention requirement set forth in section VII. The Effective Date for this CAP shall be calculated in accordance with paragraph 15 of the Resolution Agreement.

IV. Time

Any reference to number of days refers to number of calendar days. 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 Federal 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

ISU agrees to the following:

A. Hybridization.

1. ISU shall provide HHS with documentation designating it a hybrid entity and identifying all of its components that have been designated covered health care components within 30 days of the Effective Date.

B. Risk Management.

1. ISU shall provide HHS with its most recent risk management plan that includes specific security measures to reduce the risks and vulnerabilities to a reasonable and appropriate level for all of its covered health care components. ISU shall provide the risk management plan to HHS within 30 days of the Effective Date for review and approval.

2. Upon receiving notice from HHS either approving or specifying any required changes, ISU shall make the required changes accordingly and promptly implement the risk management plan, including any applicable training, in accordance with its applicable administrative procedures.

C. Information System Activity Review.

1. ISU shall provide HHS with documentation of implementation of its policies and procedures regarding information system activity review across all of its covered health care component clinics. ISU shall provide the documentation to HHS within 60 days of the Effective Date for review and approval.

2. Upon receiving any required changes to such implementation from HHS, ISU shall have 30 days to revise its implementation strategy and provide it to HHS for review and approval. ISU shall provide documentation of implementation, including any applicable training, within 30 days of receipt of HHS' approval.

D. Compliance Gap Analysis.

1. ISU shall provide documentation of its updated compliance gap analysis activity entitled *Post Incident Risk Assessment,* as specified by HHS, indicating changes in compliance status regarding each Security Rule provision. Such documentation shall include, but is not limited to, a copy of the contingency plan and the documents implementing the contingency plan as well as a listing of all technical safeguards implemented and the documents implementing the technical safeguards, across its covered health care component clinics, within 30 days of the Effective Date.

E. Reportable Events.

1. For a period of two (2) years from the Effective Date of this Agreement (the "Reporting Period"), ISU shall, upon receiving information that a workforce member may have failed to comply with its Privacy and Security policies and procedures, promptly investigate the matter. If ISU, after review and investigation, determines that a member of its workforce has failed to comply with its Privacy and Security policies and procedures, ISU shall notify HHS in writing within 30 days from the date ISU made 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 ISU's Privacy and Security policies and procedures implicated; and

    b. A description of the actions taken and any further steps ISU plans to take to address the matter, to mitigate any harm, and to prevent it from recurring, including the application of appropriate sanctions against workforce members who failed to comply with its Privacy and Security policies and procedures.

2. If no Reportable Events have occurred within the two (2) year Reporting Period, ISU shall so inform HHS in writing within thirty (30) days of the conclusion of the Reporting Period.

VI. Annual Reports

The one-year period beginning on the Effective Date and the following one-year period during the course of the period of compliance obligations shall be referred to as "the Reporting Periods." ISU shall submit to HHS Annual Reports with respect to the status of and findings regarding ISU's compliance with this CAP for each of the two Reporting Periods. ISU shall submit each Annual Report to HHS no later than 60 days after the end of each corresponding Reporting Period. The Annual Report shall include:

A. A summary of the risk management plan and security measures (addressed in section V.B.) taken during the Reporting Period, including documentation of training related to those measures;

B. A summary of the information system activity review measures (addressed in section V.C.) taken during the Reporting Period, including documentation of training related to those measures;

C. An update of the compliance gap analysis activity (addressed in section V.D.) conducted during the Reporting Period;

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

E. An attestation signed by an officer of ISU attesting that he or she has reviewed the Annual 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

ISU shall maintain for inspection and copying by HHS all documents and records relating to compliance with this CAP for six years.

VIII. Breach Provisions

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

A. Timely Written Requests for Extensions. ISU 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 days prior to the date by which any act is due to be performed or any notification or report is due to be filed. It is within HHS' sole discretion as to whether to grant or deny the extension requested.

B. Notice of Breach and Intent to Impose CMP. The Parties agree that a breach of this CAP by ISU constitutes a breach of the Resolution Agreement. Upon a determination by HHS that ISU has breached this CAP, HHS may notify ISU of (a) ISU's breach; and (b) HHS' intent to impose a civil money penalty (CMP) pursuant to 45 C.F.R. Part 160 for the Covered Conduct set forth in paragraph 3 of the Resolution Agreement and any other conduct that constitutes a violation of the HIPAA Privacy and Security Rules (this notification is hereinafter referred to as the "Notice of Breach and Intent to Impose CMP").

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

1. ISU 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) ISU has begun to take action to cure the breach; (ii) ISU is pursuing such action with due diligence; and (iii) ISU has provided HHS with a reasonable timetable for curing the breach.

D. Imposition of CMP. If at the conclusion of the 30 day period, ISU fails to meet the requirements of section VIII.C. to HHS' satisfaction, HHS may proceed with the imposition of a CMP against ISU pursuant to 45 C.F.R. Part 160 for the Covered Conduct set forth in paragraph 3 of the Resolution Agreement and any other conduct that constitutes a violation of the HIPAA Privacy and Security Rules. HHS shall notify ISU in writing of its determination to proceed with the imposition of a CMP.

For Idaho State University

_____ _____

Arthur C. Vailas, President
Idaho State University

Date

For United States Department of Health and Human Services

_____ _____

Linda Yuu Connor
Regional Manager, Region X
Office for Civil Rights

Date