Amended and Restated Effective July 1, 2014
University of Colorado Health and Welfare Plan and Trust
HIPAA Security Policy

A. Introduction

The University of Colorado Health and Welfare Plan ('H&W Plan') is sponsored by The Regents of the University of Colorado, a body corporate and a state institution of higher education of the State of Colorado ('University') and contains the following component self-funded benefits which are funded through the University of Colorado Health and Welfare Trust ('Trust'):

1. CU Health Plan- Access Network *(Membership frozen. Only available to subscribers who were subscribers as of June 30, 2010 who have continuously subscribed.)*;
2. CU Health Plan – High Deductible;
3. CU Health Plan- Exclusive;
4. Health Risk Assessment Program;
5. CU Health Plan- Kaiser;
6. CU Health Plan – Vision;
7. CU Health Plan- Medicare; and
8. CU Health Plan- Extended.

In addition, the Trust is the funding vehicle for the following plan:

9. Health Care Flexible Spending Account Component of The University of Colorado Flexible Benefits Plan ('University Flex Plan') which is sponsored by the University.

For purposes of this Security Policy, the plans listed above are referred to collectively and singularly as the "Plan." The participating employers in the Plan are the University, University of Colorado Hospital Authority ("UCH"), and University Physicians, Incorporated ("UPI") (collectively, the "Employers"). The participating employers in the University Flex Plan are the University and UPI.

Members of the Plan Sponsor's workforce may create, receive, maintain, or transmit electronic protected health information (as defined below) on behalf of the Plan Sponsor, for plan administration functions. The Plan is administered by third-party administrators and has one or more business associates that perform functions for the Plan. A list of the members of the workforce who may have access to PHI will be maintained and is listed in Exhibit A.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act) and their

implementing regulations and guidance require the Plan to implement various security measures with respect to electronic protected health information (electronic PHI).

Electronic Protected Health Information is protected health information that is transmitted by or maintained in electronic media.

Protected Health Information (PHI) is the information that is subject to and defined in the Plan's privacy policies and procedures. For purposes of this Policy, PHI does not include the following, referred to in this Policy as "Exempt Information":

(1) summary health information, as defined by HIPAA's privacy rules, for purposes of (a) obtaining premium bids or (b) modifying, amending, or terminating the Plan;

(2) enrollment and disenrollment information concerning the Plan which does not include any substantial clinical information;

(3) PHI disclosed to the Plan and/or Plan Sponsor under a signed authorization that meets the requirements of the HIPAA privacy rules; or

(4) information disclosed to Plan Sponsor by an individual for functions that Plan Sponsor performs in its role as an employer and not in its role as Plan Sponsor or in providing administrative services to the Plan.

Electronic Media means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet, intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

It is the Plan's policy to comply fully with the requirements of HIPAA's security regulations.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, or covered dependents) are intended to be created by this Policy. The Plan Sponsors, in conjunction with the Trust, reserve the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent that this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Plan, the Plan Sponsors or Trust. This Policy does not address requirements under state law or federal laws other than HIPAA. However, if the state law or other federal laws are stricter than HIPAA security regulations, the state and/or other federal laws must be followed.

I. Security Official

Chirag Joshi is the Security Official for the Plan. The Security Official is responsible for the development and implementation of the Plan's policies and procedures relating to security, including but not limited to this Policy.

II. Risk Analysis

The Plan has no employees. All of the Plan's functions, including creation and maintenance of its records, are carried out by employees of the Plan Sponsor and by business associates of the Plan. The Plan does not own or control any of the equipment or media used to create, maintain, receive, and transmit electronic PHI relating to the Plan, or any of the facilities in which such equipment and media are located. Such equipment, media, and facilities are owned or controlled by the Plan Sponsor, the third-party administrator and other business associates. Accordingly, the Plan Sponsor and business associates create and maintain all of the electronic PHI relating to the Plan, own or control all of the equipment, media, and facilities used to create, maintain, receive, or transmit electronic PHI relating to the Plan, and control their employees, agents, and subcontractors who have access to electronic PHI relating to the Plan. The Plan has no ability to assess or in any way modify any potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI relating to the Plan. That ability lies solely with the respective Plan Sponsor, the third-party administrators and other business associates.

Because the Plan has no access to or control over the employees, equipment, media, facilities, policies, procedures, or documentation of the Plan Sponsor, the third-party administrator and other business associates affecting the security of the Plan's electronic PHI; and because the Plan Sponsor, the third-party administrators and other business associates have undertaken certain obligations relating to the security of electronic PHI that they handle in relation to the performance of administrative functions for the Plan, the Plan's policies, and procedures, including this Policy, do not separately address the following standards (including the implementation specifications associated with them):

- security management process;
- workforce security;
- information access management;
- security awareness and training;
- security incident procedures;
- contingency plan;
- evaluation;
- facility access controls;
- workstation use;
- workstation security;
- device and media controls;
- access control;

- audit controls;
- integrity;
- person or entity authentication; and
- transmission security.

The HIPAA security policies and procedures of the Plan Sponsor, the third-party administrators and other business associates for electronic PHI of the Plan for the standards listed above are adopted by the Plan.

III. Risk Management

The Plan relies on the Plan Sponsor, its third-party administrators, and other business associates to manage risks to its electronic PHI by limiting vulnerabilities, based on risk assessments, to a reasonable and appropriate level, taking into account the following:

- their size, complexity, and capabilities;
- their technical infrastructure, hardware, software, and security capabilities;
- the costs of security measures; and,
- the criticality of the electronic PHI potentially affected and the probability of the various risks.

Based on risk assessments undertaken by the Plan Sponsor, the Plan's third-party administrators and the Plan's other business associates, the Plan made a reasoned, well-informed and good-faith determination on the implementation of the HIPAA security regulations that it need not take any additional security measures, other than the measures set forth herein and the measures of the Plan Sponsor, the third-party administrators, and other business associates, to reduce risks to the confidentiality, integrity and availability of electronic PHI.

IV. Plan Document

The Plan document shall include provisions requiring the Plan Sponsor to:

- implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the Plan Sponsor creates, receives, maintains, or transmits on behalf of the Plan (the Plan's electronic PHI);
- ensure that reasonable and appropriate security measures support the Plan document provisions providing for adequate separation between the Plan and the Plan Sponsor (which were adopted as described in the Plan's privacy policy);
- ensure that any agents or subcontractors to whom the Plan Sponsor provides Plan electronic PHI agree to implement reasonable and appropriate security measures to protect the Plan electronic PHI; and
- report to the Security Official any security incident of which the Plan Sponsor becomes aware.

V. Disclosures of Electronic PHI to Third-Party Administrators and Other Business Associates

A business associate is an entity (other than the Plan Sponsor), such as a third-party administrator, that creates, receives, maintains or transmits electronic PHI and:

- performs or assists in performing a Plan function or activity involving electronic PHI (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, information technology or financial services, where the performance of such services involves giving the service provider access to the Plan's electronic PHI.

The Plan permits the third-party administrators and other business associates to create, receive, maintain, or transmit electronic PHI on its behalf. The Plan has obtained or will obtain satisfactory assurances from all business associates that they will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract containing all of the requirements of the HIPAA security regulations and specifically providing that the business associate will:

- implement administrative, physical, and technical safeguards and documentation requirements that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, receives, maintains, or transmits on behalf of the Plan (the Contract electronic PHI);
- ensure that any agents or subcontractors that create, receive, maintain or transmit electronic PHI on behalf of the business associate agree to comply with all of the requirements of the HIPAA security regulations to protect the Contract electronic PHI;
- report to the Plan any security incident or breach of unsecured PHI of which the business associate becomes aware;
- take any contractually required steps with respect to breach notification requirements; and
- authorize termination of the contract by the Plan if the Plan determines that the business associate has violated a material term of the contract.

VI. Breach Notification Requirements

The Plan will comply with the requirements of the HITECH Act and its implementing regulations to provide notification to affected individuals, the Department of Health and Human Services, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

VII. Documentation

The Plan's security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental or operational changes affecting the security of Plan electronic PHI, and any changes to policies or procedures will be documented and implemented promptly.

Except to the extent that they are carried out by the Plan Sponsor or business associates, the Plan shall document certain actions, activities, and assessments with respect to electronic PHI required by HIPAA to be documented (including amendment of the Plan document in accordance with this policy, for example).

Policies, procedures, and other documentation controlled by the Plan may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

The Plan will make its policies, procedures, and other documentation available to the Security Official and the Plan Sponsor, the third-party administrators and other business associates or other persons responsible for implementing the procedures to which the documentation pertains.

APPROVED

The University of Colorado and the Trust agree to the Amended and Restated Security Policy effective as of the effective date of such amendment and restatement.

This Amended and Restated Security Policy may be executed in multiple counterparts and may be delivered by fax or other electronic means, each of which shall be deemed to be an original, and all of which together shall constitute one and the same document.

THE REGENTS OF THE UNIVERSITY
OF COLORADO, a body corporate and a state institution
of higher education of the State of Colorado

By _____ Date 12/22/14
Bruce Benson
President

UNIVERSITY OF COLORADO HEALTH AND
WELFARE TRUST

By _____ Date 1/7/15
E. Jill Pollock
Chairperson, Trust Committee

APPROVED AS TO LEGAL SUFFICIENCY
OFFICE OF UNIVERSITY COUNSEL

By _____ Date 11/11/14
Melissa Martin
Assistant University Counsel
Special Assistant Attorney General

Exhibit A
to the University of Colorado Health and Welfare Plan and Trust
HIPAA Security Policy

List of the Members of the Workforce
Who May Have Access to PHI

University of Colorado Health and Welfare Plan ('H&W Plan')

and

Health Care Flexible Spending Account Component of the University of Colorado Flexible Benefit Plan ('Health Care FSA')

Job Title/Classification

Any officer or employee of the Plan Administrator, including but not limited to personnel in the CU Health Plan Administration, who performs functions on behalf or related to administration of the H&W Plan and/or Health Care FSA, such as benefit design and administration, audit, legal, accounting and systems support

Vice President of Budget and Finance for the University of Colorado, or his or her successor

Any other employee of the University of Colorado who needs access to PHI in order to perform Plan administration functions that the Plan Sponsor performs for the H&W Plan and/or the Health Care FSA (such as quality assurance, claims processing, auditing, monitoring, payroll, and appeals (if applicable))