Amended and Restated Effective July 1, 2019
University of Colorado Health and Welfare Plan and Trust
HIPAA Privacy Policy

Table of Contents

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" or "Plan Sponsor") 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- High Deductible/HSA Compatible
2. CU Health Plan - HDHP2;
3. CU Health Plan - Exclusive;
4. CU Health Plan - Exclusive2;
5. CU Health Plan - Kaiser;
6. CU Health Plan – Vision;
7. CU Health Plan - Medicare;
8. CU Health Plan – Extended;
9. CU Health Plan - Essential Dental;
10. CU Health Plan - Choice Dental; and
11. CU Health Plan - Premier Dental

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

12. 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 Privacy 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 ("CU Medicine") (collectively, the "Employers"). The participating employers in the University Flex Plan are the University and CU Medicine.

The Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act, and their respective implementing regulations, are collectively referred to as "HIPAA" for purposes of this Privacy Policy. HIPAA restricts the Plan's ability to use and disclose protected health information. Members of the Plan Sponsor's workforce may have access to protected health information ("PHI") of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the Plan Sponsor,

for administrative functions of the Plan performed by the Plan Sponsor and other purposes permitted by the HIPAA privacy rules. A list of the members of the workforce who may have access to PHI will be maintained and is listed in Exhibit A. This Privacy Policy sets forth the Plan's policies and procedures for HIPAA compliance by the Plan and the Plan Sponsor when it receives protected health information from the Plan.

> *Protected Health Information.* Protected health information means information that is created or received by the Plan and relates to the past, present, or future physical or mental health or condition of a participant; the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

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, that is disclosed to the Plan Sponsor solely for purposes of obtaining premium bids, or modifying, amending, or terminating the Plan;
2. Enrollment and disenrollment information concerning the Plan that does not include any substantial clinical information;
3. PHI disclosed to the Plan or Plan Sponsor under a signed authorization that meets the requirements of the HIPAA privacy rules;
4. Health information related to a person who has been deceased for more than 50 years;
5. Information disclosed to the Plan Sponsor by an individual for functions that the Plan Sponsor performs in its role as an employer and not as sponsor of the Plan or in providing administrative services to the Plan.

> *Participant.* For purposes of this Privacy Policy, participant means any individual who is or has been enrolled in the Plan, including current and former employees and their dependents.

It is the Plan Sponsor's, Plan's and Trust's policy that the Plan shall comply with HIPAA's requirements for the privacy of PHI. To that end, all members of the Plan Sponsor's workforce who have access to PHI must comply with this Privacy Policy. For purposes of this Policy and the Plan Sponsor's more detailed Privacy Use and Disclosure Procedures, the workforce of the Plan Sponsor includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose work performance is under the direct control of the Plan Sponsor, whether or not they are paid by the Plan Sponsor. The term "workforce member" includes all of these types of workers.

No third-party rights in contract or otherwise (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Privacy Policy. The Plan Sponsor, in conjunction with the Trust, reserves the right to

amend or change this Policy at any time (and even retroactively) without notice. To the extent this Privacy Policy establishes requirements and obligations above and beyond those required by HIPAA, the Privacy Policy shall be aspirational and shall not be binding upon the Plan, the Plan Sponsor or Trust. This Privacy Policy does not address requirements under other federal laws or under state laws. To the extent this Privacy Policy is in conflict with the HIPAA privacy rules, the HIPAA privacy rules shall govern.

B. Plan's Responsibilities as Covered Entity

I. Privacy Official and Contact Person

The Assistant Vice President for Health Plan Compliance, CU Health Plan Administration is the Privacy Official[1] for the Plan.

The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy of the Plan's PHI, including but not limited to this Privacy Policy and the Plan's Privacy Use and Disclosure Procedures. The Privacy Official will also serve as the contact person for participants who have questions, concerns or complaints about the privacy of their PHI. The Privacy Official will coordinate the Plan's privacy activities with the Plan's Security Official.

The Privacy Official is responsible for ensuring that the Plan complies with the provisions of the HIPAA privacy rules, including the requirement that the Plan have a HIPAA-compliant Business Associate Agreement in place with all Business Associates. The Privacy Official shall also be responsible for monitoring compliance by all Business Associates with the terms of their Business Associate Agreements.

II. Workforce Training

It is the Plan Sponsor's, Plan's and Trust's policy to train all members of the workforce who have access to Plan PHI on the Plan's Policy and its Privacy Use and Disclosure Procedures. The Privacy Official is charged with developing training schedules and programs so that all workforce members receive the training necessary and appropriate to permit them to carry out their Plan functions in compliance with HIPAA. Training will be updated as necessary to reflect any changes in policies or procedures and to ensure that workforce members are appropriately aware of their obligations.

III. Safeguards and Firewall

The Plan Sponsor will establish on behalf of the Plan appropriate administrative, technical, and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements will be established. Administrative safeguards include implementing procedures for use and disclosure of PHI. See the Plan's Privacy Use and Disclosure Procedures. Technical safeguards include tracking workforce

[1] All references to Privacy Official refer to the Privacy Official or a designee.

members' access to PHI. Physical safeguards include locking filing cabinets and doors to rooms storing PHI.

Firewalls will be established to ensure that only authorized workforce members will have access to PHI. Firewalls will also ensure that workforce members have access to only the minimum amount of PHI necessary for the plan administrative functions they perform, and that they will not disclose PHI to workforce members who are not authorized to access PHI.

IV. Privacy Notice

The Privacy Official is responsible for developing and maintaining a notice of the Plan's privacy practices that complies with the HIPAA privacy rules and describes:

- the uses and disclosures of PHI that may be made by the Plan;
- the rights of individuals under HIPAA privacy rules;
- the Plan's legal duties with respect to the PHI; and
- other information as required by the HIPAA privacy rules.

The privacy notice will inform participants that the Plan Sponsor will have access to PHI in connection with its plan administrative functions. The privacy notice will also provide a description of the Plan's complaint procedures, the name and telephone number of the contact person for further information, and the effective date of the notice. The effective date will not be earlier than the date the notice is published.

The notice of privacy practices shall be placed on the Plan's or the Plan Sponsor's website. The notice also will be individually delivered:

- at the time of an individual's enrollment in the Plan;
- to a person requesting the notice; and
- to participants within 60 days after a material change to the notice. However, if the Plan posts its notice on the Plan's website and there is a material change to the notice, the Plan will prominently post the change or the revised notice on its website by the effective date of the change. It will also provide the change or information about the change and how to obtain the revised notice, in its next annual mailing to individuals covered by the Plan.

The Plan will also provide notice of availability of the privacy notice (or a copy of the privacy notice) at least once every three years in compliance with the HIPAA privacy regulations.

V. Complaints

Complaints should be addressed to:

Assistant Vice President for Health Plan Compliance
CU Health Plan Administration
1999 Broadway, Suite 820
Denver, CO 80202

The Privacy Official is responsible for creating a process for individuals to lodge complaints about the Plan's privacy procedures and for creating a system for handling such complaints. A copy of the complaint procedure shall be provided to any participant upon request. All complaints received, and their disposition, if any, will be documented.

VI. Sanctions for Violations of Privacy Policy

Sanctions against workforce members for using or disclosing PHI in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with the Plan Sponsor's discipline policy, up to and including termination of employment.

All employees of the Plan Sponsor with access to PHI of the Plan must sign the Confidentiality Agreement attached as an Appendix to this Policy.

VII. Mitigation of Inadvertent Disclosures of PHI

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it from a use or disclosure of an individual's PHI in violation of HIPAA or this Privacy Policy. As a result, if a workforce member or Business Associate becomes aware of an unauthorized use or disclosure of PHI, either by a workforce member or a Business Associate, the workforce member or Business Associate must immediately contact the Privacy Official so that appropriate steps to mitigate harm to the participant can be taken.

VIII. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No workforce member may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against participants for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No participant shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility under the Plan.

IX. Plan Document

The Plan document shall include provisions to describe the permitted and required uses and disclosures of PHI by the Plan and Trust, for plan administrative or other permitted purposes. Specifically, the Plan document shall require the Plan Sponsor to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- ensure that there is adequate separation (firewall) between the Plan and the Plan Sponsor;
- ensure that any agents to whom it provides PHI agree to the same restrictions and conditions that apply to the Plan Sponsor;
- not use or disclose PHI for employment-related actions or for any other benefit or employee benefit plan of the company;
- report to the Privacy Official any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Plan participants, consider their requests for amendments and, upon request, provide them with an accounting of PHI disclosures in accordance with the HIPAA privacy rules;

- make the Plan Sponsor's internal practices and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services (HHS) upon request;
- if feasible, return or destroy all PHI received from the Plan that the Plan Sponsor still maintains in any form and retain no copies of such information when no longer needed for the purpose for which disclosure was made, except that, if such return or destruction is not feasible, limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

The Plan document must also require the Plan Sponsor to (1) certify to the Privacy Official that the Plan documents have been amended to include the above restrictions and that the Plan Sponsor agrees to those restrictions; and (2) provide adequate firewalls in compliance with the HIPAA privacy rules.

X. Documentation

The Plan's privacy policies and procedures shall be documented and maintained for at least six years from the date last in effect. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations), as well as any changes in the Plan's operations or operating environment. Any changes to policies or procedures must be promptly documented and incorporated into workforce training.

The Plan shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The Plan shall also document the dates, content and attendance of employees at training sessions.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. The Plan will maintain such documentation for at least six years.

C. Policies on Use and Disclosure of PHI

I. Use and Disclosure Defined

The Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use*. The sharing, employment, application, utilization, examination, or analysis of PHI by any Plan Sponsor workforce member working for or within CU Health Plan Administration or by a Business Associate of the Plan.

- *Disclosure*. The release, transfer, provision of access to, or divulging in any other manner of PHI to persons who are not Plan Sponsor workforce members working within CU Health Plan Administration or to a person or entity who is not a Business Associate of the Plan.

II. Workforce Must Comply with Plan's Policy and Procedures

All members of the workforce of the Plan Sponsor who have access to PHI must comply with this Privacy Policy and with the Plan's Privacy Use and Disclosure Procedures, which are set forth in a separate document.

III. Permitted Uses and Disclosures for Plan Administration Purposes

The Plan may disclose Exempt Information to the Plan Sponsor. Exempt Information is not governed by this Policy, and the Plan Sponsor may disclose it for any lawful purpose.

The Plan may disclose PHI to certain Plan Sponsor workforce members (or classes of workforce members) listed on Exhibit A ("workforce members with access") to perform Plan administrative functions.

Workforce members with access may disclose PHI to other workforce members with access for plan administrative functions (but the PHI disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Workforce members with access may not disclose PHI to workforce members (other than workforce members with access) unless a valid, signed authorization is in place or the disclosure otherwise is in compliance with this Privacy Policy and the Plan's Privacy Use and Disclosure Procedures. Workforce members with access must take all appropriate steps to ensure that the PHI is not disclosed, available, or used for employment purposes. For purposes of this Policy, "plan administrative functions" include the payment and health care operation activities described in section C.IV of this Policy.

IV. Permitted Uses and Disclosures: Payment and Health Care Operations

PHI may be disclosed for the Plan's own payment purposes, and PHI may be disclosed to another covered entity for the payment purposes of that covered entity.

Payment. Payment includes activities undertaken to obtain participants' contributions to the Plan or to determine or fulfill the Plan's responsibility to obtain or provide reimbursement for health care. Payment also includes the following:

- eligibility and coverage determinations including coordination of benefits and adjudication or subrogation of health benefit claims;
- risk adjusting based on enrollee status and demographic characteristics;
- billing, claims management, collection activities, obtaining payment under a contract for re-insurance (including stop-loss insurance and excess loss insurance) and related health care data processing, and
- any other payment activity permitted by the HIPAA privacy regulations.

PHI may be disclosed for purposes of the Plan's own health care operations. PHI may be disclosed to another covered entity for purposes of the other covered entity's quality assessment and improvement, case management, or health care fraud and abuse detection programs, if the other covered entity has (or had) a relationship with the participant and the PHI requested pertains to that relationship.

Health Care Operations. Health care operation means any of the following activities:

- conducting quality assessment and improvement activities;
- reviewing health plan performance;
- underwriting and premium rating;
- conducting or arranging for medical review, legal services and auditing functions;
- business planning and development;
- business management and general administrative activities; and
- other health care operations permitted by the HIPAA privacy regulations.

V. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the Plan Sponsor's "non-health plan" benefits (e.g., disability, workers' compensation, life insurance, etc.), unless the participant has provided an authorization for such use or disclosure (as discussed in "Disclosures Pursuant to an Authorization") or such use or disclosure is required or allowed by applicable state law and applicable requirements under HIPAA are met.

VI. Mandatory Disclosures of PHI

A participant's PHI must be disclosed, in accordance with Plan's Privacy Use and Disclosure Procedures, in the following situations:

- The disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Information and Request for Amendment" that follows);
- The disclosure is required by law; or
- The disclosure is made to HHS for purposes of enforcing HIPAA.

VII. Other Permitted Disclosures of PHI

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Plan's Privacy Use and Disclosure Procedures describe specific requirements that must be met before these types of disclosures may be made. The requirements include prior approval of the Plan's Privacy Official. Permitted are disclosures:

- about victims of abuse, neglect or domestic violence;
- to a health care provider for treatment purposes;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- for cadaveric organ-, eye- or tissue-donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and

- that relate to workers' compensation programs.

VIII. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

IX. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used, disclosed or requested, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use, disclosure or request.

The "minimum-necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to HHS;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. The Plan, when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary for the requestor is disclosed. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All disclosures not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. The Plan, when requesting PHI subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Plan is requested. More details on the requirements are found in the Plan's Privacy Use and Disclosure Procedures. All requests not discussed in the Plan's Privacy Use and Disclosure Procedures must be reviewed on an individual basis with the Privacy Official to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

X. Disclosures of PHI to Business Associates

Workforce members may disclose PHI to Business Associates and allow Business Associates to create, receive, maintain or transmit PHI on the Plan's behalf. However, prior to doing so, the Plan must first obtain satisfactory assurances from the Business Associate, in the form of a Business Associate Agreement, that it will appropriately safeguard PHI. The Privacy Official shall maintain a log of all Business Associates and shall maintain all Business Associate Agreements in a readily accessible and retrievable form and format. Before sharing PHI with a

Business Associate, workforce members must contact the Privacy Official and verify that a Business Associate Agreement is in place.

Business Associate is an entity that:

- creates, receives, maintains or transmits PHI on behalf of the Plan (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 PHI.

XI. Disclosures of De-Identified Information

The Plan may freely use and disclose information that has been "de-identified" in accordance with the HIPAA privacy regulations. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

XII. Breach Notification Requirements

The Plan will comply with the requirements of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") and its implementing regulations to provide notification to affected individuals, HHS, and the media (when required) if the Plan or one of its business associates discovers a breach of unsecured PHI.

B. Policies on Individual Rights

I. Access to PHI and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Plan (or its Business Associates) maintains in designated record sets. A participant's personal representative may request access to PHI on behalf of the participant. The Plan will provide access to PHI in accordance with HIPAA.

Designated Record Set is a group of records maintained by or for the Plan that includes:

- the enrollment, payment, and claims adjudication record of a participant that is maintained by or for the Plan; or
- other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

Participants will be instructed to send their requests to the Plan's Privacy Official. The Plan will take reasonable efforts to verify the identity of the requesting participant following procedures approved by the Privacy Official. The Plan will attempt to provide participants with access to their PHI as soon as possible, and within 30 days, after receiving a written request. If the Plan is unable to provide access within 30 days, it may extend the response by up to 30

additional days so long as it communicates the reason for the extension to the participant and the estimated response date within the initial 30-day period.

The Plan will send requested information in the Designated Record Set to a third party identified by the participant, so long as the request is signed and in writing, and clearly identifies the third party and where to send the information.

Generally, the Plan will not deny participants access to their own PHI. However, if an exception to the right to access set forth in 45 CFR §164.524 exists, the Privacy Official will review the request for access and will respond within the timeframe and with the information required by the privacy rule.

If information in one or more Designated Record Sets is maintained electronically, and an individual requests an electronic copy of the information, the Plan will provide the individual with access to the requested information in the electronic form and format requested by the individual, if it is readily producible in that form and format. If the requested information is not readily producible in that form and format, the requested information will be produced in a readable electronic form and format as agreed by the Plan and the individual. If the Plan and the individual are unable to agree on an electronic form and format, the Plan will provide a paper copy of the information to the individual.

The Plan will send information to the participant by mail or email, as requested by the participant. However, if a participant asks to receive a copy of PHI by unencrypted email, the Plan will provide a brief warning to the participant that there is some level of risk that the participant's PHI could be read or otherwise accessed by a third party while in transit, and confirm that the participant still wants to receive PHI by unencrypted email. If the participant says yes, the Plan will comply with the request. Because of the security risk, the Plan will not copy information onto participant supplied storage media.

If a participant requests a copy of information in a Designated Record Set, the Plan may impose a reasonable, cost-based fee, provided that the fee includes only the cost of (1) labor for copying the information requested by the participant, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media if the participant requests that the electronic copy be provided on portable media; and (3) postage, when the participant has requested that the copy be mailed. If the participant agrees to receive an explanation or summary, the Plan may charge for preparing the explanation or summary, if the participant agrees in advance. The Plan may not charge a fee to participants who merely request access to but not copies of information.

II. Amending PHI

If a participant believes that PHI about the participant in a Designated Record Set is incorrect or incomplete, the participant may ask the Plan to amend the PHI. The participant has the right to request an amendment for as long as the information is kept by or for the Plan. The request for amendment must be made in writing and submitted to the Plan's Privacy Official. In addition, the participant must provide a reason that supports the request. The Plan may deny the

request for an amendment if it is not in writing or does not include a reason to support the request.

The Plan will act on the request as soon as possible, and within 60 days, after receiving the request. If the Plan is unable to act on the request within 60 days, it may extend the period for up to 30 additional days, provided that the Plan notifies the participant of the reason for the delay and the date it will act on the request during the original 60-day period.

In addition the Plan may deny the request if the request is to amend information that –

- was not created by the Plan, unless the participant provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;
- is not part of a Designated Record Set;
- is not subject to the right of access described above; or
- is accurate and complete.

If the Plan denies the request, it will provide the participant with a written explanation of the basis for the denial, the participant's right to file a statement of disagreement with the Plan, and the Plan's complaint procedures. Any future disclosures of the disputed information will include that statement.

III. Accounting

A participant has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the most recent six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure;
- pursuant to an authorization;
- to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- to correctional institutions or law enforcement when the disclosure was permitted without authorization;
- as part of a limited data set;
- for specific national security or law enforcement purposes; or
- disclosures that occurred prior to the compliance date.

Participants shall be instructed to send their requests for an accounting to the Plan's Privacy Official. The Plan shall respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure (or a copy of the written request for disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the disclosure.

The first accounting in any 12-month period shall be provided free of charge. The Privacy Official may impose reasonable production and mailing costs for additional accountings.

IV. Requests for Confidential Communications

Participants may ask to receive communications regarding their PHI by alternative means or alternative locations. For example, participants may request that Plan information be sent only to their work address rather than a home address, or may request that communications be made by phone. Participants will be instructed to send their requests to the Privacy Official. The decision to honor a request shall be made by the Privacy Official.

V. Requests for Restrictions on Use and Disclosure of PHI

A participant may request restrictions on the use and disclosure of the participant's PHI. For example, a participant can ask that the Plan not use or disclose information about a surgery that the participant had. Participants will be instructed to send their requests to the Privacy Official. The Plan may, but need not, honor such requests. However, the Plan will comply with a restriction request if (1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and (2) the PHI pertains solely to a health care item or service for which the health care provider involved has been paid in full by the individual or another person, other than the Plan. The decision to honor restriction requests shall be made by the Privacy Official.

Exhibit A
University of Colorado Health and Welfare Plan and Trust
HIPAA Privacy 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 perform 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

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))

Appendix to Privacy Policy Employee Confidentiality Agreement

I, _____, have read and understand the Privacy Policy of the University of Colorado Health and Welfare Plan and Trust, including the health care flexible spending account components of The University of Colorado Flexible Benefits Plan, for the protection of the privacy of individually identifiable health information (or protected health information [PHI]), as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition, I acknowledge that I have received training in the Plan's policies concerning PHI use, disclosure, storage, transmission and destruction as required by HIPAA.

In consideration of my employment or compensation by the Plan Sponsor as an employee or other workforce member, I hereby agree that I will not at any time—either during my employment or association with the Plan Sponsor or Plan or after my employment or association ends—use, access, transmit or disclose PHI to any person or entity, internally or externally, except as is required and permitted in the course of my duties and responsibilities with the Plan Sponsor, as set forth in the Plan's privacy policies and procedures or as permitted under HIPAA. I understand that this obligation extends to any PHI that I may acquire during the course of my employment or association with the Plan Sponsor or the Plan, whether in oral, written or electronic form and regardless of the manner in which access was obtained.

I understand and acknowledge my responsibility to apply the Plan's policies and procedures during the course of my employment or association. I also understand that any unauthorized use, acquisition, transmission or disclosure of PHI will result in disciplinary action, up to and including the termination of employment or association with the Plan Sponsor and the imposition of civil penalties and criminal penalties under applicable federal and state law, as well as disciplinary sanctions as appropriate.

I understand that this obligation will survive the termination of my employment or end of my association with the Plan Sponsor, regardless of the reason for such termination.

Signed: _____ Date: _____

APPROVED

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

This Amended and Restated Privacy 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, as PLAN SPONSOR

By DocuSigned by: Tony DeCrosta 5C1239510A8428... Date 8/13/2019

Tony DeCrosta
Associate Vice President
Chief Plan Administrator

UNIVERSITY OF COLORADO HEALTH AND WELFARE TRUST

By DocuSigned by: Kathy Nesbitt 7B698FBDDA2E450... Date 8/15/2019

Kathy Nesbitt
Chairperson, Trust Committee

APPROVED AS TO LEGAL SUFFICIENCY
OFFICE OF UNIVERSITY COUNSEL

By DocuSigned by: Melissa Martin B4146CF86C15499... Date 8/13/2019

Melissa Martin
Associate University Counsel
Special Assistant Attorney General