PLAN AMENDMENT

University of Denver Health & Welfare Benefit Plan

Plan Sponsor: University of Denver (Employer)

Effective Date of Change: February 16, 2026

Date of Notice: April 1, 2026

Reason for Update: New protections for Protected Health Information (PHI) related to substance use disorder (SUD)

As of the Effective Date of Change, University of Denve (Employer) hereby adopts this Amendment to the University of Denver Health & Welfare Benefit Plan (Plan) to reflect changes to the Plan. Pursuant to Section 5.05 of the Plan document ("Plan Amendments"),the Employer shall have the right, at any time, to modify, alter or amend the Plan. This Amendment is intended to provide good faith compliance with 42 C.F.R. Part 2 ("Confidentiality of Substance Use Disorder Patient Records") and related guidance until the Plan is formally restated to incorporate such provisions.

Plan Changes

Notwithstanding any provision contained in the Plan to the contrary, the Plan is amended as follows:

Section	Changes
Section 5.19. ("PRIVACY AND SECURITY")	Section 5.19 to the Plan document is hereby replaced in its entirety with the attached new Section 5.19 ("PRIVACY AND SECURITY") (**Attachment 1**) The Section 5.19 contained in **Attachment 1** to this Amendment shall supersede any prior versions of the Plan's Section 5.19.

All other Plan provisions remain unchanged so long as they are consistent with this Plan Amendment.

IN WITNESS WHEREOF, the undersigned authorized representative has adopted this Amendment to the Plan as of the Effective Date above, on behalf of University of Denver to evidence the adoption of this Amendment as set forth herein.

For University of Denver

Signature: 

Signer's Name: Lloyd Moore

Signer's Title: Director of Benefits

Date Signed: 03/05/2026

5.19 PRIVACY AND SECURITY

To the extent that any Plan Component is a group health plan that uses, creates, maintains, or has access to Protected Health Information ("PHI"), including Substance Use Disorder PHI ("SUD PHI") governed by the HIPAA Privacy, Security, and Breach Notification Rules and the regulations implementing 42 C.F.R. Part 2, as amended by the 2024 Final Rule effective February 16, 2026, all such Plan Components intend to operate in accordance with those requirements. The Plan Sponsor's HIPAA Privacy Procedures, HIPAA Security Procedures, HIPAA Breach Notification Procedures, Substance Use Disorder PHI Confidentiality Procedures, and any other privacy and security documents related to these procedures are incorporated by reference herein.

A. General – Except for a Health Care Plan Component that is self-administered and has fewer than 50 Participants, the Plan Component will be operated in accordance with HIPAA and the corresponding regulations, as amended from time to time, including the HIPAA-aligned requirements applicable to Substance Use Disorder ("SUD") records protected under 42 C.F.R. Part 2 ("Part 2"), to the extent such records are created, received, maintained, or transmitted by the Plan

B. HIPAA and Part 2 Privacy Standards

1. The authorized representative of the Plan shall not disclose PHI to any member of the Employer's workforce unless each of the conditions set out in this Plan Section 5.19 (B) are met. For SUD records subject to Part 2, the Plan shall additionally comply with the consent, redisclosure, and notice obligations applicable to Part 2 PHI ("SUD PHI"), except to the extent such requirements have been aligned with HIPAA pursuant to the 2024 Part 2 Final Rule.

2. PHI disclosed to members of the Employer's workforce shall be used or disclosed by them only for purposes of Plan administrative functions. The Plan's administrative functions shall include all Plan payment functions and health care operations. The terms "payment" and "health care operations" shall have the same definitions as set forth in the Privacy Standards, but the term "payment" generally shall mean activities taken to determine or fulfill Plan responsibilities with respect to eligibility, coverage, provision of benefits, or reimbursement for health care. If the persons to whom information is disclosed violate this Plan Section 5.19 (B), or applicable law or regulation, the Plan shall cease disclosing such information.

   Use or disclosure of SUD PHI shall also comply with Part 2's limitations on redisclosure, and any redisclosure shall include the required Part 2 prohibition-on-redisclosure notice unless otherwise permitted under the revised regulations.

3. The Plan shall disclose PHI only to members of the Employer's workforce who are authorized to receive such PHI, and only to the extent and in the minimum amount necessary for that person to perform their duties with respect to the Plan. "Members of the Employer's workforce" shall refer to all employees and other persons under the Employer's control. The Employer shall keep an updated list of those authorized to receive PHI.

   Members of the Employer's workforce with access to SUD PHI must also receive training on the confidentiality requirements under Part 2 and the restrictions on redisclosure applicable to SUD PHI

4. Authorized members of the Employer's workforce who receive PHI shall use or disclose the PHI only to the extent necessary to perform their duties with respect to the Plan. This includes compliance with any additional limitations on SUD PHI under Part 2.

5. In the event that any member of the Employer's workforce uses or discloses PHI other than as permitted by this Section 5.19 and the HIPAA Privacy Rule, and corresponding regulations, the incident shall be reported to the Plan's Privacy Officer. In addition, the Privacy Officer and the Employer must take the following steps:

   a. The Privacy Officer must

      i. investigate the incident to determine whether the breach occurred inadvertently, through negligence, or deliberately; whether there is a pattern of breaches; and the degree of harm caused by the breach;

      ii. make appropriate sanctions against the persons causing the breach, which, depending upon the nature of the breach, may include oral or written reprimand, additional training, or termination of employment;

      iii. mitigate any harm caused by the breach, to the extent practicable;

      iv. document the incident and all actions taken to resolve the issue and mitigate any damages; and

      v. if the breach involves SUD PHI, comply with the breach notification requirements applicable to Part 2 PHI as integrated into the HIPAA Breach Notification Rule under the 2024 Final Rule.

   b. The Employer must provide certification to an authorized representative of the Plan that it agrees to

      i. not use or further disclose the information other than as permitted or required by the Plan or as required by law;

      ii. ensure that any agent or subcontractor, to whom it provides PHI received from the Plan, agrees to the same restrictions and conditions that apply to the Employer with respect to such information;

      iii. not use or disclose PHI for employment-related actions and decisions or in connection with any other benefit or employee benefit plan of the Employer;

      iv. report to the Plan any use or disclosure of the PHI of which it becomes aware that is inconsistent with the uses or disclosures permitted by this Section 5.19or required by law;

      v. make available PHI to individual Plan members in accordance with HIPAA Privacy Rule section 164.524;

vi. make available PHI for amendment by individual Plan members and incorporate any amendments to PHI in accordance with HIPAA Privacy Rule section 164.526;

vii. make available the PHI required to provide an accounting of disclosures to individual Plan members in accordance with HIPAA Privacy Rule section 164.528;

viii. make its internal practices, books, and records relating to the use and disclosure of PHI received from the Plan available to the Department of Health and Human Services for purposes of determining compliance by the Plan with the HIPAA Privacy Rule;

ix. return or destroy (if feasible) all PHI received from the Plan that the Employer 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;

x. ensure the adequate separation between the Plan and members of the Employer's workforce, as required by HIPAA Privacy Rule section 164.504(f)(2)(iii), and

xi. with respect to SUD PHI, comply with all mandatory nondiscrimination provisions, consent requirements, redisclosure restrictions, and patient-rights obligations under Part 2 as aligned with HIPAA.

6. Failure to comply with the terms of this Plan Section 5.19 (B) shall be resolved by persons entitled to use or disclose PHI in a timely manner. Violations involving SUD PHI shall also be evaluated under applicable Part 2 enforcement provisions.

C. HIPAA Electronic Security Standards.

If this Plan is subject to the Security Standards for the Protection of Electronic PHI (HIPAA Privacy Rule Parts 160, 162, and 164, the "Security Standards"), then this Plan Section 5.19 (C) shall apply as follows:

1. The Employer agrees to implement reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of Electronic PHI that the Employer creates, maintains, or transmits on the Plan's behalf. "Electronic PHI" shall have the same definition as set out in the Security Standards, but generally shall mean PHI that is transmitted by or maintained in electronic media. This includes SUD PHI that is maintained or transmitted in electronic form.
2. The Employer shall ensure that any agent or subcontractor to whom it provides Electronic PHI shall agree, in writing, to implement reasonable and appropriate security measures to protect the Electronic PHI.
3. The Employer shall ensure that reasonable and appropriate security measures are implemented to comply with the conditions and requirements described in this Plan Section 5.19 (C).
4. The Employer will report to the Plan any security incident under the Security Standards of which it becomes aware.
5. The Employer will establish reasonable and appropriate security measures to ensure adequate separation between the Plan and the Employer, in support of the requirements described in this Plan Section 5.19 (C).