



## **HIPAA Privacy Policy**

### **I. Introduction**

UnitedAg ("the Company") sponsors the following group health plans United Agricultural Benefit Trust and the UAL Flexible Benefits Plan.

For purposes of this Privacy Policy, the plans listed above are referred to collectively and singularly as the "Plan."

Members of the Company's workforce may have access to protected health information of Plan participants (1) on behalf of the Plan itself; or (2) on behalf of the Company, for administrative functions of the Plan performed by the Company and other purposes permitted by the HIPAA privacy rules.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict the Plan's and the Company's ability to use and disclose protected health information.

*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, protected health information 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 Company 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. protected health information disclosed to the Plan or the Company 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 Company by an individual for functions that the Company performs in its role as an employer and not as sponsor of the Plan or in providing administrative services to the Plan.

It is the Company's policy that the Plan shall comply with HIPAA's requirements for the privacy of protected health information. To that end, all members of the Company's workforce who have access to protected health information must comply with this Privacy Policy. For purposes of this Policy and the Plan's more detailed Privacy Use and Disclosure Procedures, the Company's workforce includes individuals who would be considered part of the workforce under HIPAA, such as employees, volunteers, contractors, trainees, and other persons whose work performance is under the direct control of the Company, whether

or not they are paid by the Company. The term "workforce member" includes all of these types of workers.

No third-party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or Business Associates) are intended to be created by this Policy. The Company reserves the right to amend or change this Policy at any time (and even retroactively) without notice. To the extent 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 or the Company. This Policy does not address requirements under other federal laws or under state laws. To the extent this Policy is in conflict with the HIPAA privacy rules, the HIPAA privacy rules shall govern.

## **II. Plan's Responsibilities as Covered Entity**

### **A. Privacy Official and Contact Person**

Clare Marie Einsmann will be the Privacy Official 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 protected health information, 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 protected health information. 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 all provisions of the HIPAA privacy rules, including the requirement that the Plan have a HIPAA-compliant Business Associate Contract in place with all Business Associates. The Privacy Official shall also be responsible for monitoring compliance by all Business Associates with the HIPAA privacy rules and the terms of their Business Associate Contracts.

### **B. Workforce Training**

It is the Company's policy to train all members of its workforce who have access to protected health information for familiarity and compliance with 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 necessary and appropriate training to permit them to carry out their Plan functions in compliance with HIPAA. Workforce 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.

### **C. Safeguards and Firewall**

The Company will establish on behalf of the Plan appropriate administrative, technical, and physical safeguards to prevent protected health information from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Administrative safeguards include implementing procedures for use and disclosure of protected health information. See the Plan's Privacy Use and Disclosure Procedures. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets.

Firewalls will ensure that only authorized workforce members will have access to protected health information, that they will have access to only the minimum amount of protected health information necessary for the plan administrative functions they perform, and that they will not further use or disclose protected health information in violation of HIPAA's privacy rules.

### **D. 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 protected health information that may be made by the Plan;
- the rights of individuals under HIPAA privacy rules;
- the Plan's legal duties with respect to the protected health information; and
- other information as required by the HIPAA privacy rules.

The privacy notice will inform participants that the Company will have access to protected health information 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 Company'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, and 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.

#### **E. Complaints**

Clare Marie Einsmann, 949.975.1424, ext. 237 will be the Plan's contact person for receiving complaints. 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.

#### **F. Sanctions for Violations of Privacy Policy**

Sanctions for using or disclosing protected health information in violation of HIPAA or this HIPAA Privacy Policy will be imposed in accordance with UAL Employee Handbook up to and including termination of employment

#### **G. Mitigation of Inadvertent Disclosures of Protected Health Information**

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 protected health information in violation of HIPAA or the policies and procedures set forth in this Policy. As a result, if a workforce member or Business Associate becomes aware of an unauthorized use or disclosure of protected health information, 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.

#### **H. 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 individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment, or eligibility under the Plan.

#### **I. Plan Document**

The Plan Document(s) shall include provisions to describe the permitted and required uses by, and

disclosures to, the Company of protected health information for plan administrative or other permitted purposes. Specifically, the Plan document shall require the Company to:

- not use or further disclose protected health information other than as permitted by the Plan documents or as required by law;
- ensure that any agents to whom it provides protected health information agree to the same restrictions and conditions that apply to the Company;
- not use or disclose protected health information 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 protected health information available to Plan participants, consider their amendments, and, upon request, provide them with an accounting of protected health information disclosures in accordance with the HIPAA privacy rules;
- make the Company's internal practices and records relating to the use and disclosure of protected health information received from the Plan available to the Department of Health and Human Services (HHS) upon request; and
- if feasible, return or destroy all protected health information received from the Plan that the Company 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.

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

#### **J. 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), and the Plan's practices and processes. Any changes to policies or procedures must be promptly documented.

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 workforce members 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.

### **III. Policies on Use and Disclosure of Protected Health Information**

#### **A. Use and Disclosure Defined**

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

- *Use*. The sharing, employment, application, utilization, examination, or analysis of protected health information by any Company workforce member working within the Benefits Department of United Agricultural Benefit Trust or of the Company, or by a Business Associate of the Plan(s).
- *Disclosure*. The release, transfer, provision of access to, or divulging in any other manner of protected health information to persons who are not Company workforce members working within the Benefits Department of United Agricultural Benefit Trust or of the Company, or to a

person or entity who is not a Business Associate of the Plan.

## **B. Workforce Must Comply With Plan's Policy and Procedures**

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

## **C. Permitted Uses and Disclosures for Plan Administration Purposes**

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

The Plan may disclose protected health information to the following Company workforce members to perform Plan administrative functions ("workforce members with access"):

- Benefit Administrator
- Claims Department
- Customer Service Department
- Administration Department
- CFO and relevant Accounting Personnel
- Legal Department

Workforce members with access may disclose protected health information to other workforce members with access for plan administrative functions (but the protected health information disclosed must be limited to the minimum amount necessary to perform the plan administrative function). Workforce members with access may not disclose protected health information 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 Policy and the Plan's Privacy Use and Disclosure Procedures. Workforce members with access must take all appropriate steps to ensure that the protected health information 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 III.D of this Policy.

## **D. Permitted Uses and Disclosures: Payment and Health Care Operations**

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

*Payment.* Payment includes activities undertaken to obtain Plan contributions or to determine or fulfill the Plan's responsibility for provision of benefits, or to obtain or provide reimbursement for health care. Payment also includes:

- 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 reinsurance (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.

Protected health information may be disclosed for purposes of the Plan's own health care operations. Protected health information 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 protected health information requested pertains to that relationship.

*Health Care Operations.* Health care operations 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.

#### **E. No Disclosure of Protected Health Information for Non-Health Plan Purposes**

Protected health information may not be used or disclosed for the payment or operations of the Company's "non-health" benefits (e.g., disability, workers' compensation, life insurance), 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 all applicable requirements under HIPAA are met.

#### **F. Mandatory Disclosures of Protected Health Information**

A participant's protected health information 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.

#### **G. Other Permitted Disclosures of Protected Health Information**

Protected health information 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.

#### **H. Disclosures of Protected Health Information Pursuant to an Authorization**

Protected health information 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.

## **I. Complying With the "Minimum-Necessary" Standard**

HIPAA requires that when protected health information 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 Protected Health Information.* The Plan, when disclosing protected health information subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of protected health information 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 Protected Health Information.* The Plan, when requesting protected health information subject to the minimum-necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of protected health information 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.

## **J. Disclosures of Protected Health Information to Business Associates**

Workforce members may disclose protected health information to the Plan's Business Associates and allow the Plan's Business Associates to create, receive, maintain, or transmit protected health information on its behalf. However, prior to doing so, the Plan must first obtain assurances from the Business Associate, in the form of a business associate contract, that it will appropriately safeguard the information. Before sharing protected health information with outside consultants or contractors who meet the definition of a "Business Associate," workforce members must contact the Privacy Official and verify that a Business Associate contract is in place.

A Business Associate is an entity that:

- creates, receives, maintains, or transmits protected health information on behalf of the Plan (including for claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services to or for the Plan, where the performance of such services involves giving the service provider access to protected health information.

## **K. 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.

## **L. Breach Notification Requirements**

The Plan will comply with the Reportable Breach Notification Policy set forth in Appendix B of this Policy.

## **IV. Policies on Individual Rights**

### **A. Access to Protected Health Information and Requests for Amendment**

HIPAA gives participants the right to access and obtain copies of their protected health information that the Plan (or its Business Associates) maintains in designated record sets. HIPAA also provides that participants may ask to have their protected health information amended. The Plan will provide access to protected health information, and it will consider requests for amendment that are submitted in writing by participants.

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

- the enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or
- other protected health information used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

If information in one or more designated record sets is maintained electronically, and an individual requests an electronic copy of such 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 such form and format; if the requested information is not readily producible in such 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 the form and format, the Plan will provide a paper copy of the information to the individual.

### **B. Accounting**

An individual has the right to obtain an accounting of certain disclosures of his or her own protected health information. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment, or health care operations;
- to individuals about their own protected health information;
- 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.

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 subsequent accountings.

### **C. Requests for Alternative Communication Means or Locations**

Participants may ask to receive communications regarding their protected health information by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. The Plan may, but need not, honor such requests. The decision to honor such a request shall be made by the Privacy Official.

However, the Plan must accommodate such a request if the participant clearly states that the disclosure of all or part of the information could endanger the participant. The Privacy Official has responsibility for administering requests for confidential communications.

### **D. Requests for Restrictions on Use and Disclosure of Protected Health Information**

A participant may request restrictions on the use and disclosure of the participant's protected health information. 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 protected health information 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.