Ohio University Health Plan

HIPAA Privacy Standards and Procedures

For Internal Use Only

Ohio University Health Plan ("Plan") reserves the right to change these Standards and Procedures at any time. These Standards and Procedures apply to protected health information generated by or on behalf of Plan; under no circumstances do these Standards and Procedures apply to disability, AD&D, life insurance, or any other non-health benefits. To the extent these Standards and Procedures express requirements and obligations above and beyond those required by the Health Insurance Portability and Accountability Act (HIPAA) privacy rules, as amended, these Standards and Procedures will be treated as goals, but will not be binding on the Plan. These Standards and Procedures do not address the requirements of any laws or regulations other than the HIPAA privacy rules. No third party rights (including, but not limited to, rights of Plan participants or business associates) are intended to be created by these Standards and Procedures.

TABLE OF CONTENTS

Ohio University Health Plan

I. Scope of the HIPAA Privacy Rules

Only *protected health information* held by, or on behalf of, a covered entity is subject to the HIPAA privacy rules.

1. Covered entities are:

    a. health care providers;

    b. health care clearinghouses; and

    c. health plans.

2. Generally, the health plans and programs subject to COBRA are health plans subject to the HIPAA privacy rules. For Ohio University Health Plan, these are medical, prescription drug, dental, vision, health flexible spending account ("Health FSA"), EAP programs, and wellness programs, as well any new programs which may be implemented from time to time and which are also subject to COBRA.

3. The HIPAA privacy rules do not apply to any disability, life insurance, or AD&D programs even though those programs have health information.

    a. However, if medical information from a provider is needed, the program may be indirectly affected by the HIPAA privacy rules. For example, a health care provider will not be able to send a medical report directly to a disability plan unless the member has signed a HIPAA-compliant authorization form.

    b. No authorization is needed if the provider gives the medical report to the member who then gives the report to the disability plan insurer or claims administrator (or even Ohio University Health Plan).

4. Protected health information is individually identifiable health information created or received by (or on behalf of) a health care provider, health care clearinghouse, or health plan.

    a. "Health information" is any information that relates to the past, present, or future physical or mental health or condition of a participant; or the past, present, or future payment for the provision of health care to a participant.

    b. Information is "individually identifiable" if it either identifies the participant or contains enough specific information to identify the participant.

OHIO UNIVERSITY

II. Retention of Documents that Demonstrate the Administration of the HIPAA Standards

While reviewing the Standards, take note that any documentation required in a Standard should be kept for a minimum of six (6) years. This guidance does not pertain to medical records with PHI. Moreover, the required documentation related to the destruction/disposal of PHI must be "permanently" retained.

If you have any questions pertaining to retention of HIPAA related records, contact the University Privacy Officer.

OHIO UNIVERSITY

III. HIPAA Standards

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

1. Permitted Uses and Disclosures

STANDARD

Protected health information may be used for treatment, payment, and Plan operations and for a limited number of other purposes as permitted or required by law.

PROCEDURES

Protected health information may be used and disclosed by or on behalf of the Plan in the following ways:

1. Protected health information may be used and disclosed for:

    a. treatment by a health care provider;

    b. payment activities (including payment activities of another health plan); and

    c. Plan operations.

    See the Notice of Privacy Practices and the Standards on Routine Use and Non-Routine Use.

2. Protected health information may be disclosed to the participant who is the subject of the information (or the participant's personal representative). See the Standards on Participant Assistance and Personal Representatives.

3. Protected health information may be disclosed to a participant's family members and other persons involved in the participant's health care. See the Notice of Privacy Practices and the Standard on Participant Assistance.

4. Protected health information may be disclosed pursuant to a participant's authorization. See the Standards on Participant Assistance and Authorizations.

5. Protected health information may be used and/or disclosed in connection with certain legal and public responsibilities. See the Notice of Privacy Practices.

Reference: 45 CFR §164.502(a)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

2. Routine Use

STANDARD

The Plan Administration Staff will use the minimum necessary protected health information in performing its routine duties with respect to Plan administration.

PROCEDURES

1. The following jobs include responsibilities for Plan administration (collectively, the "Plan Administration Staff") and may use, receive, and create protected health information as described below:

    a. Human Resources personnel supporting the Plan, including without limitation, Chief Human Resource Officer, Director of Benefits, Assistant Director of Benefits, Benefits Manager, Employee Benefits Specialists, Wellness program coordinators and staff.

    b. Information Technology personnel supporting the Plan.

    c. The following OU Department personnel supporting the Plan:

        i. Internal Audit

        ii. Payroll

        iii. Bursar's office

        iv. Legal

    d. Such other jobs as may be designated in writing from time to time by the Privacy Officer as having Plan administration responsibilities.

2. Participant assistance.

    a. Responsible staff:

        i. Human Resources personnel supporting the Plan, including without limitation, HR Service Center Specialists.

        ii. Information Technology personnel supporting the Plan, including the IT Help Desk.

b. Protected health information: A claims administrator or insurer may disclose protected health information that is related to the subject of a participant's inquiry or the inquiry of an individual who is involved in the participant's health care, to the following:

i. Human Resources personnel supporting the Plan, including without limitation, Chief Human Resource Officer, Director of Benefits, Assistant Director of Benefits, Benefits Manager, Employee Benefits Specialists, Wellness program coordinators and staff.

ii. Information Technology personnel supporting the Plan.

iii. The following OU Department personnel supporting the Plan:

a. Internal Audit
b. Payroll
c. Bursar's office
d. Legal

iv. Such other jobs as may be designated in writing from time to time by the Privacy Officer as having Plan administration responsibilities.

c. Use: Protected health information that is related to the subject of the inquiry will be used to resolve the issue(s) raised by the participant or individual making the inquiry. See the Standard on Participant Assistance.

3. Financial and administrative oversight and control.

a. Responsible staff:

i. Human Resources personnel supporting the Plan, including without limitation, Chief Human Resource Officer, Director of Benefits, Assistant Director of Benefits, Benefits Manager, Employee Benefits Specialists, Wellness program coordinators and staff.

ii. Information Technology personnel supporting the Plan.

iii. The following OU Department personnel supporting the Plan:

a. Internal Audit

b. Payroll

c. Bursar's office

d. Legal

iv. Such other jobs as may be designated in writing from time to time by the Privacy Officer as having Plan administration responsibilities.

b. Protected health information: A claims administrator may provide to

i. Human Resources personnel supporting the Plan, including without limitation, Chief Human Resource Officer, Director of Benefits, Assistant Director of Benefits, Benefits Manager, Employee Benefits Specialists, Wellness program coordinators and staff.

ii. Information Technology personnel supporting the Plan.

iii. The following OU Department personnel supporting the Plan:

a. Internal Audit

b. Payroll

c. Bursar's office

d. Legal

iv. Such other jobs as may be designated in writing from time to time by the Privacy Officer as having Plan administration responsibilities.

The following information:

(1) claims detail reports, stop loss reports, high dollar claim reports, large claim reports, and other similar reports of claims; and

(2) check registers and other reports of payments.

c. Use: The protected health information will be used to:

(1) confirm expenses;

(2) reconcile bank records;

(3) track stop-loss payments;

(4) plan and project expenditures; and

(5) monitor the performance of claims administrators.

4. Health FSA program.

a. Responsible staff:

i. Human Resources personnel supporting the Plan, including without limitation, Chief Human Resource Officer, Director of Benefits, Assistant Director of Benefits, Benefits Manager, Employee Benefits Specialists, Wellness program coordinators and staff.

ii. Information Technology personnel supporting the Plan.

iii. The following OU Department personnel supporting the Plan:

a. Internal Audit

b. Payroll

c. Bursar's office

d. Legal

iv. Such other jobs as may be designated in writing from time to time by the Privacy Officer as having Plan administration responsibilities.

b. Protected health information: Members will submit claim forms, bills for medical expenses, and explanations of benefits (EOBs) from medical plans.

c. Use: The member must submit a claim form, a bill, and (where applicable) an EOB. The personnel enumerated in 4(a)(i) above may check records of the medical flexible spending account program and/or other health plan sponsored by Ohio University. The protected health information will be used to decide the amount to be reimbursed. Checks and EOBs will be sent to the member.

5. Appeals.

a. Responsible staff:

i. Human Resources personnel supporting the Plan, including without limitation, Chief Human Resource Officer, Director of Benefits, Assistant Director of Benefits, Benefits Manager, Employee Benefits Specialists, Wellness program coordinators and staff.

ii. Information Technology personnel supporting the Plan.

iii. The following OU Department personnel supporting the Plan:

a. Internal Audit

b. Total Compensation Committee

c. Ohio University Provost

d. Legal

iv. Such other jobs as may be designated in writing from time to time by the Privacy Officer as having Plan administration responsibilities.

b. Protected health information: The claims administrator may turn over the administrative record on the denied claim and any lower-level appeal so that the appeal can be decided based on the entire record (as is required by Department of Labor rules).

c. Use: The protected health information will be used to decide the appeal.

Reference: 45 CFR §164.502(b) and §164.514(d)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

3. Non-Routine Use

STANDARD

The Plan Administration Staff will use the minimum amount of protected health information necessary to achieve the purpose of a permissible, but non-routine, use or disclosure of protected health information.

PROCEDURES

1. The Plan will rely on representations that the protected health information requested is the minimum amount necessary in the case of a non-routine request for a disclosure of protected health information from:

    a. a public official for a permitted disclosure;

    b. a health care provider;

    c. another health plan;

    d. a health care clearinghouse; or

    e. a business associate of the Plan that represents that the protected health information requested is the minimum necessary.

2. The minimum necessary standard does not apply to:

    a. disclosures to providers for treatment;

    b. disclosures to the individual who is the subject of the protected health information;

    c. disclosures pursuant to the authorization of the individual who is the subject of the protected health information;

    d. disclosures to the U.S. Department of Health and Human Services for compliance and enforcement purposes;

    e. uses or disclosures required by other laws; and

    f. uses or disclosures required for compliance with the HIPAA electronic data interchange rules.

3. For other non-routine uses and disclosures of protected health information, the request will be forwarded to the Plan's Privacy Officer (or his or her designee) to determine if the amount of protected health information requested is the minimum necessary to achieve the purpose of the disclosure according to established criteria.

4. The Plan will not disclose a participant's entire record in fulfillment of a request subject to the minimum necessary standard unless a specific justification for such a disclosure is made and documented.

Reference: 45 CFR §164.502(b) and §164.514(d)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

4. Disclosures to Ohio University Health Plan

STANDARD

Ohio University Health Plan's access to protected health information will be limited to the protected health information needed by Ohio University as Plan Sponsor for the purpose of Plan administration.

PROCEDURES

1. The Plan Administration Staff has Plan administration functions and may have access to protected health information in connection with performing those functions. A claims administrator or insurer may disclose protected health information to the Plan Administration Staff so that the Plan Administration Staff can perform its Plan administration functions.

2. Other employees of Ohio University do not have Plan administration functions. Disclosures to employees who are not employees of the Plan Administration Staff will be limited as follows:

    a. The Plan Administration Staff, a claims administrator, or an insurer may disclose enrollment information to Ohio University as Plan Sponsor (e.g., information as to whether individuals are covered by the Plan and the periods for which they are covered).

    b. The Plan Administration Staff, a claims administrator, or an insurer may provide Ohio University as Plan Sponsor with de-identified or summary health information (i.e., health information that is not individually identifiable) for the purpose of considering amendments to the Plan.

    c. The Plan Administration Staff, a claims administrator, or an insurer may disclose protected health information to Ohio University as Plan Sponsor as required to comply with applicable workers' compensation laws.

    d. The Plan Administration Staff, a claims administrator, or an insurer may disclose protected health information to Ohio University as Plan Sponsor if required by law.

    e. The Plan Administration Staff, a claims administrator, or an insurer may disclose protected health information to Ohio University as Plan Sponsor pursuant to a participant's authorization.

3. Protected health information originating with the Plan (or a claims administrator or insurer) cannot be used in connection with Ohio University Health Plan's non-health benefits or programs (e.g., disability benefits or leaves of absence) unless the participant has authorized such use. See the Standard on Authorizations.

Reference: 45 CFR §164.504(f)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

5. Business Associates

STANDARD

The Plan's business associates will be required to enter into a business associate agreement with the Plan wherein they agree to maintain the privacy of participants' protected health information and only use and disclose protected health information for the purposes for which the information was provided.

PROCEDURES

1. The Privacy Officer (or a member of the Plan Administration Staff designated by the Privacy Officer) will consider the proposed functions of each new Plan vendor to determine whether the vendor will use, disclose, create, or maintain protected health information as part of its functions for the Plan. A vendor that will use, disclose, create, or maintain protected health information as part of its functions carried out for the Plan is a business associate. A business associate agreement between the Plan and the business associate should be signed before the business associate receives protected health information related to the Plan.

2. A business associate will determine the minimum necessary type and amount of protected health information required to perform services for the Plan. The Plan may rely on the professional judgment of business associates to determine the type and amount of protected health information necessary for their purposes.

3. The Plan is required by law to notify affected individuals without unreasonable delay (and not later than 60 days) after the discovery of a Breach of unsecured protected health information. See the Breach Notification Standard.

    a. Although the Plan retains the ultimate legal responsibility for Breach notification, it may delegate tasks related to Breach notification to business associates.

    b. The Plan will work with each of its business associates to determine which tasks will be undertaken by the business associate in the event of a Breach of the protected health information that the business associate uses, discloses, creates, or maintains on behalf of the Plan. The allocation of tasks will be incorporated into the business associate agreement or otherwise memorialized so as to be available in the event of a Breach.

4. The Privacy Officer will review (or direct the review of) any complaints regarding potential privacy violations by a business associate.

    a. See the Breach Notification Standard for any complaint, inquiry, or other notice to the Privacy Officer or to any member of the Plan Administration Staff that alleges

inappropriate acquisition, access, use, or disclosure of any protected health information (an "Incident").

b. If the Privacy Officer is aware of a material violation of the business associate's duties with regard to privacy, the Privacy Officer will take reasonable steps to end the violation. If such steps are unsuccessful, the Privacy Officer will determine whether termination of the underlying services contract with the business associate is feasible.

Reference: 45 CFR §164.502(e) and §164.504(e)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

6. Participant Assistance

STANDARD

When an individual contacts the Plan Administration Staff for assistance with a Plan claim, the Plan Administration Staff member assisting the individual will take steps to verify the individual's identity and will limit the disclosures to the individual according to the individual's relationship to the participant who is the subject of the inquiry.

PROCEDURES

1. The Plan Administration Staff is always permitted to explain Plan benefits, limits, and exclusions where such explanation does not involve accessing protected health information (i.e., participant-specific claims information held by or on behalf of the Plan).

2. Plan Administration Staff will verify the identity of any individual who wants assistance with a claim or other matter involving protected health information ("customer service inquiries"). If the individual making the inquiry is not personally known to the Plan Administration Staff member, the Staff member will ask the individual for his or her name, relationship to the member, as well as the information below to confirm the identity of the individual making the inquiry:

    a. if the individual making the inquiry is the member or the member's spouse or domestic partner:

        (1) the name and last four digits of the Social Security number of the member and, at the option of the Plan Administration Staff other identifying information (e.g., the member's address, date of birth of the member, and/or the date of birth of a family member) to compare to the Plan's records; and

        (2) if the subject of the inquiry is the member's spouse, domestic partner, or other dependent, the name of the spouse, domestic partner, or dependent, and, at the option of Plan Administration Staff, other identifying information (e.g., last four digits of the Social Security number, date of birth, or address) for the spouse, domestic partner, or dependent;

    b. if the individual making the inquiry is not the member or the member's spouse or domestic partner, or the parent or legal guardian of a minor child, the Staff will generally not provide any additional information to the individual.

3. In cases where an individual is asking about his or her own claims, but another person is present (e.g., a spouse or friend), the Plan Administration Staff will confirm that the individual agrees to disclosures in the presence of the other person.

4. The Plan Administration Staff may disclose claims status information in response to customer service inquiries.

    a. Plan Administration Staff may disclose protected health information to the individual making the inquiry only if the individual can identify one or more specific claims (by, e.g., approximate date of service and/or name of provider) that are the subject of his or her question.

    b. In response to a question about the status of a specific claim, Plan Administration Staff may disclose whether the claim was received, whether the claim was paid, the amount and date of payment, and (to the extent normally disclosed on an EOB) the reason for the amount of payment, if known.

    c. In cases where an individual is asking about claims incurred by another individual, Plan Administration Staff will use professional judgment and experience with common practice to determine whether responding to the inquiry is in the best interests of the individual who is the subject of the inquiry. The specificity of the individual's questions will indicate the individual's involvement in the participant's health care. However, if deemed appropriate by Plan Administration Staff, Plan Administration Staff may instruct the individual making the customer service inquiry to have the participant who is the subject of the protected health information either (1) make the inquiry, or (2) sign an authorization.

    d. The Plan Administration Staff will not discuss medical history or any other information unrelated to the claim(s) identified by the individual making the inquiry. The individual making the inquiry may be referred to a claims administrator, insurer, and/or a provider for additional information.

Reference: 45 CFR §164.510(b) and §164.514(h)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

7. Personal Representatives

STANDARD

The personal representative of a participant generally has the same rights as the participant to the participant's protected health information.

PROCEDURES

1. If an individual requesting the disclosure of protected health information identifies himself or herself as a personal representative of an unemancipated minor, the Plan Administration Staff will ask about the individual's relationship to the minor.

    a. If the individual confirms that he or she is:

        (1) a parent, guardian, or other person acting in loco parentis; and

        (2) in control of making health care decisions for the minor, then he or she may be treated as the minor's personal representative (except if the care involves mental health, substance abuse, family planning, or sexually transmitted diseases).

    b. If the care involves mental health, substance abuse, family planning, or sexually transmitted diseases, Plan Administration Staff shall seek direction from the Privacy Officer prior to making the disclosure.

2. If an individual requesting the disclosure of protected health information identifies himself or herself as a personal representative of an adult or emancipated minor or has authority to review records under Ohio's power of attorney statute, the Plan Administration Staff will not make any disclosure, and will request documentation of personal representative status (e.g., a Power of Attorney or Letter of Guardianship). Upon receipt of the requested documentation, the Privacy Officer will review the documentation provided and determine its sufficiency for purposes of any disclosure.

3. The Plan will treat the administrator or executor of a deceased participant's estate as a personal representative.

4. The Plan Administration Staff will make a record of the identity of the personal representative and maintain the supporting documentation.

5. Notwithstanding the above, the Plan may elect not to treat a person as the personal representative of a participant if it is reasonable to believe that the participant has been or may be subjected to domestic violence, abuse, or neglect by such person, or if treating such person as the personal representative could endanger the participant, and/or the Plan Administration Staff determines that it is not in the best interests of the participant to treat such person as a personal representative.

Reference: 45 CFR §164.502(g)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

8. Authorizations

STANDARD

A participant may authorize the Plan to disclose his or her protected health information to any person and/or for any purpose.

PROCEDURES

1. If a participant wants the Plan Administration Staff to disclose protected health information to a specific person or entity not within the scope of the Standard on Participant Assistance, the participant will need to sign an authorization. See also Routine Use Standard.

2. The participant may revoke the authorization, in writing, at any time.

3. If the participant does not want the Plan Administration Staff to be involved in the disclosure, the participant should submit the authorization to the claims administrator or insurer holding the records that are the subject of the authorization.

4. If a participant submits an authorization to the Plan Administration Staff, the Plan Administration Staff will keep the original and forward a copy (or keep a copy and forward the original) of the authorization to the claims administrator or insurer holding the records that are the subject of the authorization.

5. The Plan Administration Staff will keep authorizations and revocations of authorizations for at least six (6) years after they are created, expired, or revoked, whichever date is later. See Standard regarding Document Retention.

6. Ohio University as Plan Sponsor will require that each of the Plan's claims administrators, with respect to records maintained by that claims administrator on behalf of the Plan, will:

    a. track participants' authorizations and revocations of authorizations; and

    b. retain authorizations and revocations of authorizations for at least six (6) years after they are created, expired, or revoked, whichever date is later.

Administrative Form: Authorization Form

Reference: 45 CFR §164.508(b) and (c)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

9. Requests for Confidential Communications

STANDARD

Participants have the right to request that the Plan communicate with them in a confidential way if standard communications would endanger them.

PROCEDURES

Plan

1. The Plan's claims administrators, on behalf of the Plan and in accordance with the HIPAA privacy rules, will consider and accept or reject participants' requests for confidential communications related to protected health information maintained by that claims administrator on behalf of the Plan.

2. A participant's request for confidential communications that is submitted to the Plan Administration Staff will be promptly forwarded to the appropriate claims administrator.

3. The claims administrator (acting on behalf of the Plan) will normally mail a family's EOBs to the member at the member's home address.

    a. If a participant does not want his or her EOBs and/or other information mailed to the member's home address, the participant may submit a request to the claims administrator for confidential communications at an alternative address (or by an alternative means).

    b. The claims administrator will grant the participant's request if the request is reasonable and the participant asserts that the standard method or form of communication would endanger him or her.

4. Certain Plan Administration Staff and claims administrators will provide customer service to the member, the member's spouse or domestic partner, and other involved individuals concerning claims status for all covered family members. See the Standard regarding Participant Assistance.

    a. The member's access to family members' claims information cannot be limited due to the nature of family coverage (including deductibles and out-of-pocket maximums).

    b. Otherwise, if a participant does not want family members and involved individuals to be able to discuss the participant's claims information with:

(1) the Plan Administration Staff, the participant may submit instructions to the Plan Administration Staff to have this access stopped.

(2) a claims administrator, the participant may submit instructions to the claims administrator to have this access stopped.

c. Such a request will generally be honored:

(3) if the participant making the request is an adult; or

(4) if the request is made by the parent of a minor dependent and does not relate to access of the other parent.

5. All documentation evidencing the Plan's agreement to confidential communications requested by participants will be maintained for at least six (6) years.

Health FSA

1. The Plan Administration Staff or a claims administrator will mail all EOBs, checks, and/or other communications regarding the Health FSA to the member at the member's home address. Because claims for members of a family unit can only be submitted by and paid to the member (and not the spouse or a dependent of the member), written communications cannot be diverted to a spouse or child.

2. Certain Plan Administration Staff and the claims administrator (acting on behalf of the Health FSA) will provide customer service to both the member and his or her spouse concerning claims status for members of a family unit. See the Standard regarding Participant Assistance. If an member does not want a family member to be able to discuss claims information with the Plan Administration Staff or claims administrator, the workforce member may submit a request to the Plan Administration Staff or claims administrator, as applicable, to have this access stopped. Such requests will be granted.

a. Members should submit requests for confidential communications in writing to the Privacy Officer (for Plan Administration Staff) or the claims administrator.

b. The Privacy Officer or claims administrator, in accordance with the HIPAA privacy rules, will consider and accept or reject members' requests for confidential communications related to protected health information maintained by the Plan Administration Staff or claims administrator on behalf of the Health FSA.

3. All documentation evidencing the Health FSA's agreement to confidential communications requested by members will be maintained by the Privacy Officer or claims administrator (acting on behalf of the Health FSA) for at least six (6) years. See the Standard regarding Document Retention.

Administrative Form: Request for Confidential Communications Form

Reference: 45 CFR §164.510(b) and §164.522(b)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

10. Requests for Restrictions

STANDARD

Participants have the right to request restrictions on how their protected health information is used and/or disclosed for treatment, payment, and Plan operations.

PROCEDURES

1. A participant's request for restrictions on the use and/or disclosure of his or her protected health information must be submitted in writing to the Privacy Officer.

    a. The Privacy Officer will consider the administrative burdens on the Plan in determining whether to grant or deny a request for a restriction.

    b. The Privacy Officer may consult with any business associates (including the claims administrator) if the restriction might affect the business associates' use and/or disclosure of protected health information.

2. When a request for restrictions is accepted by the Privacy Officer:

    a. The participant will be informed of any potential consequences of the restriction;

    b. A notation will be made in the participant's record;

    c. The Privacy Officer will notify affected business associates of the restriction;

    d. The use and/or disclosure of protected health information will be consistent with the status of the restriction in effect on the date it is used or disclosed;

    e. The participant will be informed that the Plan is not required to comply with the agreed upon restriction(s) in emergency treatment situations when the restricted protected health information is needed for treatment; and

    f. If the agreed upon restriction hampers treatment, the Plan will ask the participant to modify or revoke the restriction and get written agreement to the modification or revocation or document an oral agreement.

3. When a request for restrictions is denied by the Privacy Officer:

    a. The participant will be given the opportunity to discuss his or her privacy concerns, if desired; and

    b. Efforts will be made to assist the participant in modifying the request for restrictions to accommodate his or her concerns and obtain acceptance by the Plan.

4. Ohio University Health Plan will require that each of its claims administrators, on behalf of the Plan and in accordance with the HIPAA privacy rules, consider and accept or reject participants' requests for restrictions related to their protected health information contained in the records maintained by that claims administrator on behalf of the Plan.

5. Any participant requests for restrictions that are submitted to the Plan Administration Staff will be promptly forwarded to the Privacy Officer and/or appropriate claims administrator.

Administrative Form: Request for Restrictions Form

Reference: 45 CFR §164.522(a)

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

11. Requests for Access

STANDARD

Participants have the right to inspect or obtain a copy of their protected health information in the designated record set maintained by the Plan or its business associates.

PROCEDURES

1. Participant requests for access to protected health information should be submitted in writing to the Privacy Officer.

2. When a written request for access to protected health information is received, it will be acted upon (a) within thirty (30) days, if the requested information is maintained and accessible on site; or (b) within sixty (60) days, if the requested information is maintained off site.

3. The time frames stated above may be extended one time for no more than thirty (30) days. If the extension is necessary, the Privacy Officer will provide the participant, within the time frames above, a written notice that specifies the reason(s) for the delay and the date by which the participant may expect to receive a decision on the request to access the protected health information for inspection and/or copying.

4. The Privacy Officer will coordinate with claims administrators (and, if relevant, other vendors) to collect the records subject to the request.

5. The Plan will grant access to protected health information maintained by the Plan or its business associates for which there are no grounds to deny access.

6. The Plan will deny access to psychotherapy notes and information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding.

7. When a request for access is accepted (in whole or in part):

    a. The participant will be notified of the decision;

    b. The participant may choose to inspect the protected health information, copy it, or both, in the form or format requested;

    c. In lieu of providing access, the Plan may provide a summary of the requested protected health information for an additional charge if the participant agrees to the summary and to the additional fee;

d. The Plan and the participant will arrange a mutually convenient time and place for the participant to inspect and/or obtain a copy of the requested protected health information; and

e. The Plan will mail a copy of the requested protected health information if the participant prefers this method of obtaining a copy.

f. Access to protected health information, if any, maintained electronically will be provided to the participant consistent with the HIPAA privacy rules.

8. Fees charged by the Plan for access to protected health information:

a. The Plan may charge a reasonable, cost-based fee for copying, including labor and supplies (e.g., paper, computer disks);

b. The Plan may charge the cost of postage when the participant requests that the information be mailed;

c. No fee is charged for retrieving or handling the protected health information or for processing the participant's access request; and

d. The Plan may charge a nominal fee for preparing an explanation or summary of the requested protected health information if the participant is informed of and agrees to receive a summary of the protected health information and is willing to pay the fee.

9. When the Plan denies a request for access (in whole or in part):

a. The participant will be given a statement explaining:

(1) the reasons for the denial;

(2) a description of how the participant may file a complaint with the Plan, including the title and telephone number of a Plan contact person; and

(3) a description of how the participant may file a complaint with the Department of Health and Human Services.

b. If the Plan does not maintain the protected health information requested but knows where the requested protected health information is maintained, the Plan will inform the participant of where to direct the request.

10. The protected health information of a deceased participant will be maintained and protected on the same basis as a participant's protected health information. A personal representative of the deceased participant (someone with legal authority to act on behalf of the deceased

participant or his or her estate) may exercise the deceased participant's rights with respect to protected health information.

11. Ohio University Health Plan will require that each of the Plan's claims administrators, on behalf of the Plan and in accordance with the HIPAA privacy rules, consider and accept or reject participants' requests for access to their protected health information contained in the records maintained by that claims administrator on behalf of the Plan.

12. Any participant requests for access related to records maintained by a claims administrator that are submitted to the Plan Administration Staff will be promptly forwarded to the appropriate claims administrator.

13. Any participant requests for access related to insured benefits that are submitted to the Plan Administration Staff will be promptly forwarded to the appropriate insurer.

Administrative Form: Request for Access to Protected Health Information Form

Reference: 45 CFR §164.524

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

12. Requests for Amendments

STANDARD

Participants have the right to request amendment of incorrect or incomplete protected health information contained in the designated record set.

PROCEDURES

1. A participant's request for amendment of his or her protected health information must be submitted in writing to the Privacy Officer and must include a reason to support acceptance of the amendment.

2. When a request for amendment of protected health information is received, it will generally be acted upon within sixty (60) days. If the Privacy Officer cannot respond within this time frame, the Privacy Officer may take an extension of up to thirty (30) days. The participant requesting the amendment will be informed in writing of the reason(s) for the delay and the date by which action will be taken on the request. The extension notice will be provided within sixty (60) days of receipt of the original request.

3. A request for an amendment will be denied if the protected health information which is the subject of the participant's request:

    a. was not created by the Plan, unless the participant provides a reasonable basis to believe that the originator of protected health information is no longer available to act on the requested amendment;

    b. is not part of the Plan's records; or

    c. is accurate and complete.

4. When a request for amendment is granted (in whole or in part), the Plan will:

    a. identify the record(s) that are the subject of the amendment request and will append the amendment to the record(s);

    b. inform the participant that his or her request for amendment has been accepted and request the identification of and permission to contact other individuals or health care entities that need to be informed of the amendment(s); and

c. make reasonable efforts to provide the amendment within a reasonable time to the persons/entities identified by the participant as well as persons and business associates that the Plan knows have the disputed protected health information and may rely on it to the participant's detriment.

5. When a request for amendment is denied:

a. The Privacy Officer will notify the participant, in writing, of the denial. The notice will include:

(1) the basis for denial;

(2) an explanation of the participant's right to submit a statement of disagreement and how to file the statement;

(3) a statement that, if the participant does not file a statement of disagreement, the participant may request that the Plan provide the request for amendment and the denial in any future release of the disputed protected health information; and

(4) a description of the procedure to file a complaint with the Plan or the Department of Health and Human Services.

b. If the participant chooses to write a statement of disagreement with the denial decision:

(1) The Plan may write a rebuttal statement and will provide a copy to the participant; and

(2) The Plan will include the request for amendment, denial letter, statement of disagreement, and rebuttal (if any) with any future disclosures of the disputed protected health information.

c. If the participant does not choose to write a statement of disagreement with the denial decision, the Plan is not required to include the request for amendment and denial decision letter with future disclosures of the disputed protected health information unless requested by the participant.

6. When the Plan receives notification from another Covered Entity that a participant's protected health information has been amended, the Plan will:

a. ensure that the amendment is appended to all applicable records of the participant; and

b. inform its business associates that may use or rely on the participant's protected health information of the amendment and require them to make the necessary corrections.

7. Any participant requests for amendment related to insured benefits that are submitted to the Plan Administration Staff will be promptly forwarded to the appropriate insurer.

8. Ohio University Health Plan will require that each of the Plan's claims administrators, on behalf of the Plan and in accordance with the HIPAA privacy rules, consider and accept or reject participants' requests for amendments to their protected health information contained in the records maintained by that claims administrator on behalf of the Plan.

9. Any participant requests for amendment related to records maintained by a claims administrator that are submitted to the Plan Administration Staff will be promptly forwarded to the appropriate claims administrator.

Administrative Form: Request to Amend Protected Health Information Form

Reference: 45 CFR §164.526

Ohio University Health Plan

HIPAA Privacy Standard and Procedures:

13. Requests for an Accounting

STANDARD

Participants have the right to request an accounting of the disclosures of their protected health information (excluding disclosures made for treatment, payment, and Plan operations and any other disclosures excepted from the accounting requirement by the HIPAA privacy rules).

PROCEDURES

1. A participant may receive an accounting of disclosures once during any twelve (12) month period free of charge.

2. If a participant requests more than one accounting within the same twelve (12) month period, a reasonable, cost-based fee may be charged by the Plan. The participant will be informed of the fee in advance and will be provided the opportunity to modify or withdraw the request.

3. No accounting will be made for disclosures of a participant's protected health information that the Plan made:

   a. more than six (6) years prior to the date of the participant's request;

   b. for the purpose of treatment, payment, or Plan operations;

   c. to the participant, the participant's personal representative, or persons involved in the participant's health care; or

   d. pursuant to the participant's authorization.

4. The accounting will generally be limited to disclosures:

   a. for public health activities;

   b. to report abuse, neglect, or domestic violence;

   c. for health oversight activities (e.g., a disclosure to the Department of Labor in the course of an audit);

   d. as required in connection with judicial and administrative proceedings (including Qualified Medical Child Support Orders and National Medical Support Notices);

e. to a public official for law enforcement purposes;

f. concerning decedents to coroners, medical examiners, or funeral directors;

g. related to organ and tissue donation;

h. for research;

i. to avert a serious threat to health or safety;

j. for specialized government functions relating to military personnel;

k. for workers' compensation; and

l. for an intentional or unintentional violation of the HIPAA privacy rules unless the individual has been notified under the applicable breach notification Standard.

5. When a written request for an accounting of disclosures of protected health information is received, it will generally be acted on within sixty (60) days. If the Privacy Officer cannot respond within this time frame, the Privacy Officer may take an extension of up to thirty (30) days. The participant requesting the accounting will be informed in writing, within sixty (60) days of the original request, of the reason(s) for the delay and the date by which action will be taken upon the request.

6. The accounting for each disclosure will include:

a. the date of the disclosure;

b. the name of the entity or person to whom the disclosure was made and its address (if known);

c. a brief description of the protected health information disclosed; and

d. one of the following:

(1) a brief statement of the purpose of the disclosure; or

(2) a copy of the written request for the disclosure from a governmental agency.

7. Notwithstanding the foregoing, if the accounting includes multiple disclosures to the same person/entity for a single purpose, the accounting will include only the frequency or number of disclosures and the date of the last disclosure made during the accounting period for all disclosures after the first disclosure.

8. Any participant requests for an accounting related to records of insured benefits that are submitted to the Plan Administration Staff will be promptly forwarded to the appropriate insurer.

9. Ohio University Health Plan will require that each of the Plan's claims administrators respond, on behalf of the Plan and in accordance with the HIPAA privacy regulations, to participants' requests for an accounting of disclosures of their protected health information in the designated record set maintained by that claims administrator on behalf of the Plan.

10. Any participant requests for an accounting related to records maintained by a claims administrator that are submitted to the Plan Administration Staff will be promptly forwarded to the appropriate claims administrator.

Administrative Form: Request for an Accounting Form

Reference: 45 CFR §164.528

OHIO UNIVERSITY HEALTH PLAN

HIPAA Privacy Standard and Procedures:

14. Complaints

STANDARD

Participants may complain to the Privacy Officer or the U.S. Department of Health and Human Services if they believe that their privacy rights have been violated.

PROCEDURES

1. Complaints to the Privacy Officer must be made in writing, 160 West Union Street, Office 150, Athens, Ohio 45701. and include:

    a. the name, address, and last four digits of the Social Security number of the complainant (and the member, if the complainant is a family member of the member); and

    b. a description of the acts or omissions believed to be in violation of the HIPAA privacy rules and/or the Plan's Notice of Privacy Practices.

2. The Privacy Officer will investigate a complaint and notify the complainant of his or her findings.

3. The complainant may also file his or her complaint with the U.S. Department of Health and Human Services.

4. No retaliatory action will be taken against participants who file complaints.

5. Documentation of all complaints received by the Health Plan, and their disposition, will be maintained for at least six (6) years.

6. See the Standard on Breach Notification for any complaint, inquiry or other notice to the Privacy Officer or to any member of the Plan Administration Staff that alleges inappropriate acquisition, access, use or disclosure of protected health information (an "Incident").

Reference: 45 CFR §160.306 and §164.530(a), (d), and (g)

OHIO UNIVERSITY HEALTH PLAN

HIPAA Privacy Standard and Procedures:

15. Privacy Officer

STANDARD

The Privacy Officer will oversee compliance with the HIPAA privacy rules, the Plan's Notice of Privacy Practices, and the HIPAA Standards and procedures.

PROCEDURES

1. Ohio University Health Plan will designate a Privacy Officer for the Plan.

2. The Privacy Officer (or his or her designee) will:

   a. determine which employees and/or departments of Ohio University have job responsibilities related to Plan administration that involve the use of protected health information. See the Standard on Routine Use.

   b. determine the level of access to protected health information that those workforce members and/or departments need to perform their job responsibilities. See the Standard on Routine Use.

   c. determine the minimum amount of protected health information needed to achieve the purpose of routine disclosures. See the Standard on Routine Use.

   d. review certain non-routine uses and/or disclosures of protected health information to determine whether the amount of protected health information requested is the minimum necessary to achieve the purpose of the disclosure. See the Standard on Non-Routine Use.

   e. serve as a contact person for participants who have questions or concerns about the privacy of their protected health information or who want to request confidential communications, restrictions, access, amendments, and/or accountings. See the Standards on Requests for Confidential Communications, Requests for Restrictions, Requests for Access, Requests for Amendments, and Requests for an Accounting.

   f. investigate participant complaints alleging violations of the HIPAA privacy rules, the Plan's Notice of Privacy Practices, and the Plan's HIPAA Standards and procedures. See the Standard on Complaints.

   g. determine, on a case-by-case basis, in consultation with the University's Privacy Officer appropriate mitigation and sanctions to apply in the event of an workforce member's

violation of the HIPAA privacy regulations, the Plan's Notice of Privacy Practices, or the Plan's HIPAA Standards and procedures. See the Standard on Mitigation and Sanctions.

Reference: 45 CFR §164.530(a)(1)

OHIO UNIVERSITY HEALTH PLAN

HIPAA Privacy Standard and Procedures:

16. Notice of Privacy Practices

STANDARD

The privacy practices of the Plan will be described in the Plan's Notice of Privacy Practices.

PROCEDURES

1. The Notice of Privacy Practices may be distributed (one copy per family unit), as required by the HIPAA privacy rules, to:

   a. all current participants who request it; and

   b. to all new participants in connection with enrollment in the Plan.

2. The Plan will post the Notice of Privacy Practices on its website or otherwise, as consistent with the HIPAA privacy rules.

3. The Notice of Privacy Practices may be incorporated into the summary plan description for the Plan.

4. The Notice of Privacy Practices will be revised as needed to reflect any changes in the HIPAA Privacy rules and the Plan's privacy practices.

5. If there is a material change to the Notice of Privacy Practices, the Plan will prominently post a revised Notice of Privacy Practices by the effective date of the material change to the Notice, and provide the revised Notice of Privacy Practices in its next annual mailing to all members who are participants in the Plan.

6. At least once every three (3) years, the Plan will notify members who are participants of the availability of the Notice of Privacy Practices and provide instructions on obtaining a copy.

7. The Privacy Officer will retain copies of the original Notice of Privacy Practices and any subsequent revisions for a period of at least six (6) years from the date it was last in effect.

Reference: 45 CFR §164.520(b) and (c)

OHIO UNIVERSITY HEALTH PLAN

HIPAA Privacy Standard and Procedures:

17. Firewall

STANDARD

The Plan will reasonably safeguard protected health information from any intentional or unintentional use or disclosure in violation of the HIPAA privacy rules.

PROCEDURES

1. Protected health information will be stored, transferred, and disposed of by the Plan by methods reasonably intended to prevent unintended disclosure.

2. If an Ohio University employee is not a member of the Plan Administration Staff, he or she will not be permitted to access protected health information except as otherwise permitted in the Notice of Privacy Practices and the HIPAA privacy rules. Access may be limited by Standards and procedures, training, physical controls (e.g., locked cabinets or rooms), and/or electronic controls (such as passwords on computer systems).

3. The Plan Administration Staff will take reasonable measures to keep visitors and other third parties from viewing protected health information on desks, in files, on printers or faxes, or on computer screens.

4. If a participant comes to the Plan Administration Staff to discuss a matter involving protected health information and other employees who are not part of the Plan Administration Staff are present, the member of the Plan Administration Staff who assists the participant will offer the option to move to a private space or room so that the conversation is less likely to be overheard by others.

5. When assisting a participant over the telephone, a member of the Plan Administration Staff will limit what he or she says about the participant so as to minimize incidental disclosures to other employees in the vicinity.

6. If the offices or other workspaces of members of the Plan Administration Staff will be accessed after hours by janitorial, repair, or other persons who are not members of the Plan Administration Staff and no member of the Plan Administration Staff will be present:

    a. Plan Administration Staff members will take reasonable measures to avoid leaving protected health information in plain view (e.g., on paper or computer screens);

    b. Plan Administration Staff members will sign off (or use screen savers) so that protected health information cannot be accessed on the computer without a password; and

c. Paper files with protected health information will be held in locked drawers, cabinets, or rooms.

Reference: 45 CFR §164.530(c)

OHIO UNIVERSITY HEALTH PLAN

HIPAA Privacy Standard and Procedures:

18. Training

STANDARD

All workforce members who need access to participants' protected health information to perform Plan administrative functions will receive training on privacy protections.

PROCEDURES

1. All members of the Plan Administration Staff will receive annual training on the Plan's Notice of Privacy Practices and the Plan's HIPAA Standards and procedures.

    a. Current members of the Plan Administration staff will receive annual HIPAA compliance training.

    b. New employees who are part of the Plan Administration Staff will receive HIPAA compliance training as part of their initial training.

2. If an Ohio University Health Plan's HIPAA privacy Standard or procedure is materially changed, or the HIPAA privacy rules materially change, affected members of the Plan Administration Staff will receive retraining related to the applicable change.

3. The Privacy Officer will maintain documentation of privacy training for at least six (6) years.

Reference: 45 CFR §164.530(b)

OHIO UNIVERSITY HEALTH PLAN

HIPAA Privacy Standard and Procedures:

19. Document Retention

STANDARD

The Plan will retain paper or electronic copies of certain documentation relating to the creation, maintenance, use, and/or disclosure of protected health information, as required by the HIPAA privacy rules[1].

PROCEDURES

1. The claims administrators, other vendors acting on behalf of the Plan, and/ or the Plan Administration Staff shall retain paper or electronic copies of the following documents for a minimum period of six (6) years from the date the document was created or was last in effect, whichever is later, or for a longer period if so required by applicable law:

2. Documentation of personal representative status for an adult or emancipated minor. See the Standard on Personal Representatives.

3. Signed authorizations and revocations of authorizations. See the Standard on Authorizations.

4. Documentation evidencing the Plan's agreement to confidential communications requested by participants. See the Standard on Requests for Confidential Communications.

5. Documentation evidencing the Plan's agreement to restrictions requested by participants, including a record of the privacy protections and/or restrictions agreed to by the Plan, and any revocation of such privacy protections and/or restrictions. See the Standard on Requests for Restrictions.

6. Designated record sets subject to access by individual participants, requests for access by individual participants, and the Plan's treatment of such requests, if any. See the Standard on Requests for Access.

7. Requests by participants for amendments to protected health information, and the Plan's disposition of such requests. See the Standard on Requests for Amendments.

8. Information required to be included in an accounting of the Plan's uses and/or disclosures of protected health information, requests for accountings by participants, and the

[1] General Rule for Retention: 1. for minors: retain to the minor's age of majority plus six (6) years; 2. for adults: retain for six (6) years unless longer period required by IUC retention rules.

accountings actually provided to participants. See the Standard on Requests for an Accounting.

9. Complaints received by the Plan, and their disposition. See the Standard on Complaints.

10. Documentation evidencing training (and periodic retraining) of members of the Plan Administration Staff. See the Standard on Training.

11. Documentation of discipline applied against members of the Plan Administration Staff (or any other workforce members) for failure to comply with the HIPAA Privacy rules, the Plan's Notice of Privacy Practices, and/or the Plan's HIPAA Standards and procedures. See the Standard on Mitigation and Sanctions.

12. The Plan's HIPAA Standards and procedures, as revised from time to time.

13. Other written correspondence and other documentation relating to the documents expressly required to be retained by this Standard to which prudent business practices dictate that the Plan retain paper or electronic copies of such documentation in accordance with this Standard and procedure.

Reference: 45 CFR §164.530(j)

OHIO UNIVERSITY HEALTH PLAN

HIPAA Privacy Standard and Procedures:

20. Mitigation and Sanctions

STANDARD

The Plan will apply appropriate sanctions against any employee who violates its privacy practices.

PROCEDURES

1. If a member of the Plan Administration Staff knows or suspects that an employee of Ohio University Health Plan or a business associate of the Plan has used or disclosed protected health information in a way that violates the HIPAA privacy rules, the Plan's Notice of Privacy Practices, or the Plan's HIPAA Standards and procedures, he or she will notify the Plan Privacy Officer and the University Privacy Officer.

2. The Privacy Officer will direct, to the extent practicable, mitigation of the harmful effects of a violation of which he or she becomes aware.

3. Sanctions will be applied against any workforce member who violates the HIPAA privacy rules, the Plan's Notice of Privacy Practices, or the Plan's HIPAA Standards and procedures.

    a. The University Privacy Officer will determine, on a case-by-case basis, appropriate sanctions based on the nature of the violation, its severity, and whether it was intentional or unintentional.

    b. Sanctions will be imposed in accordance with Ohio University's employee discipline process, including but not limited to retraining, verbal warnings, written warnings, probationary periods, and/or termination of employment.

4. No sanctions will be applied against an employee (including Plan Administration Staff) as a result of filing a complaint regarding any actual or potential violations of the HIPAA privacy rules, the Plan's Notice of Privacy Practices, or the Plan's HIPAA Standards and procedures.

5. Any sanctions applied will be documented and retained for a period of at least six (6) years.

Reference: 45 CFR §164.530(e) and (f)

OHIO UNIVERSITY HEALTH PLAN

HIPAA Privacy Standard and Procedures:

21. Breach Notification

STANDARD

The Plan will notify affected individuals without unreasonable delay (and not later than sixty (60) days) after the discovery of a Breach of unsecured protected health information.

PROCEDURES

1. PHI held by the Plan. The Plan Administration Staff must be able to identify the systems and physical locations where PHI is held by the Plan.

    a. For ePHI, the Plan Administration Staff will identify servers, databases, e-mail systems, and any other system that may contain ePHI. For each item, identify the points at which the information is Encrypted (e.g., at rest or during transmission), if any. See the Appendix for a definition of "Encryption."

    b. For all other PHI (e.g. paper), identify the physical locations such as desks, records centers and file rooms.

    c. PHI may be held in other locations with the knowledge and prior consent of a Plan Administration Staff member.

    d. Document retention/destruction Standards apply, subject to the HIPAA privacy rules.

2. Business associates using PHI on behalf of the Plan.[2]

    a. See the Business Associates Standard for Breach notification provisions to consider in the negotiation of business associate agreements.

    b. The Plan Administration Staff must keep a record of business associates along with a record (typically, as part of the business associate agreement) of the allocation of duties with respect to Breach notification for each business associate.

    c. If the Breach involves unsecured PHI under the control of a business associate, the business associate must notify the Plan of the Breach:

[2] A business associate is required to notify a covered entity of a "breach." 45 CFR 164.410. Therefore, unless the business associate agreement provides otherwise, the business associate decides whether an inappropriate use or disclosure of PHI it holds for the Plan is in fact a Breach as defined in 45 CFR §164.402.

(1) without unreasonable delay (and no later than sixty (60) days) after the business associate's discovery of the Breach (45 CFR §164.410); or

(2) if sooner, the date specified in the business associate agreement.

d. The Plan may delegate Breach notification responsibilities to its business associates. If the Plan delegates Breach notification responsibilities to a business associate and that business associate fails to fulfill its responsibilities, the Plan is required to resume those responsibilities.

3. Incident detection and reporting.

a. The Plan should have reasonable systems in place to detect Breaches. See the Plan's HIPAA Security Standards and Procedures.

b. If a Plan Administration Staff member receives a complaint, inquiry, or other notice, or otherwise becomes aware of a suspected inappropriate acquisition, access, use or disclosure of PHI (an "Incident"), the Plan Administration Staff member will promptly report the Incident to the Privacy Officer.

4. Investigation.

a. The Plan Privacy Officer in consultation with the University Privacy Officer will assign one or more members of the Plan Administration Staff to investigate each Incident.

b. The assigned Plan Administration Staff member(s) will collect information on:

(1) the circumstances surrounding the Incident;

(2) the date the Incident occurred and date it was discovered;

(3) the identity and number of individuals whose information was involved; and

(4) the type of PHI and/or other information involved (e.g., name, address, Social Security number).

5. Evaluation.

The assigned Plan Administration Staff member(s), the Privacy Officer, and the Legal Department or outside counsel will evaluate whether the Incident is a Breach. See the Appendix for the definition of "Breach." If the Incident is a Breach, the Breach notification rules apply. Such evaluation will generally consider the following issues:

a. Determine whether all of the information was secured when it was the subject of the Incident. See the Appendix for details on the requirements that must be met in order for information to be considered Secured.

(1) If yes, the Breach notification rules do not apply to the Incident.

(2) If no, the Breach notification rules may apply to the Incident.

b. Determine whether any of the three exceptions for accidental workforce errors apply. See the Appendix for details.

(1) If yes, the Breach notification rules do not apply to the Incident.

(2) If no, the Breach notification rules may apply to the Incident.

c. Determine whether there is a low probability that PHI was compromised as a result of the Incident. See the Appendix for details of the mandatory risk assessment.

(1) If yes (i.e., low probability of compromise), the Breach notification rules do not apply to the Incident.

(2) If no (i.e., not a low probability that PHI was compromised), the Breach notification rules apply to the Incident.

6. <u>If the Breach notification rules do not apply to the Incident</u>:

a. <u>Document the evaluation process</u>. The Incident is presumed to be a Breach unless demonstrated otherwise in a comprehensive, written risk analysis.

b. <u>Reduction of the risk of future Incidents</u>.

(1) Evaluate the Plan's HIPAA Standards and procedures to determine if changes are needed in light of the Incident or to decrease the possibility of future similar incidents.

(2) Determine whether additional training is needed in light of the Incident or to decrease the possibility of future similar incidents.

7. <u>If the Breach notification rules apply to the Incident</u>:

a. <u>Individual notices</u>.

(1) Timing. The Plan Administration Staff (or a business associate) must give notice to impacted individuals without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of the Breach.

A Breach is "discovered" on the first day on which such Breach is known to the Plan or its business associate (including any person, other than the individual committing the Breach, that is an employee, officer or other agent or subcontractor of the Plan or business associate) or should reasonably have been known to the Plan or business associate (or person) to have occurred.

(2) Form. The Plan Administration Staff (or a business associate) must send written notice via first class mail. The Plan (or a business associate) can send notice via e-mail in lieu of first class mail only if the individual has agreed to e-mail notices.

(a) If there is an imminent danger of misuse of the information, also contact the affected individuals by telephone, e-mail or other means. Paper/e-mail notice is still required.

(3) Insufficient contact information.

(a) The Plan Administration Staff should consult with legal counsel regarding any impacted individuals for whom there is insufficient contact information or if notices are returned as undeliverable. Substitute notice is required.

(b) In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall:

(I) be in the form of either a conspicuous posting for a period of ninety (90) days on the home page of the Plan's website, or conspicuous notice in major print or broadcast media in geographic areas where the impacted individuals are likely reside; and

(II) include a toll-free phone number that remains active for at least ninety (90) days where an individual can learn whether the individual's unsecured PHI may be included in the Breach.

(4) Content. The notice will include:

(a) a description of what happened;

(b) the date the Breach occurred and date it was discovered;

(c) the type of PHI involved (e.g., name, address, Social Security number);

(d) steps individuals can take to protect themselves;

(e) steps the Plan is taking to investigate, mitigate the harm and avoid future Breaches; and

(f) contact information.

b. Media notice of large Breach. If a Breach affects more than 500 individuals, the Plan must inform prominent media outlets (e.g., via press release). The timing and content are the same as for the individual notices.

c. Notice to HHS.

(1) All notices of Breaches are reported to the Department of Health and Human Services (HHS) at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

(2) If a Breach affects 500 or more individuals (all states), the timing and content of the notice to HHS are the same as for the individual notices.

(3) If a Breach affects fewer than 500 individuals, it must be reported to HHS within sixty (60) days after the end of the calendar year in which the breach occurred (i.e., by March 1).

d. Reduction of the risk of future Incidents.

(1) Evaluate the Plan's HIPAA Standards and procedures to determine if changes are needed in light of the Incident or to decrease the possibility of future similar incidents.

(2) Determine whether additional training is needed in light of the Incident or to decrease the possibility of future similar incidents.

Appendix: Breach Notification – Definitions

Reference: ARRA §13402 [42 USC §17932], 45 CFR 164 Subpart D

OHIO UNIVERSITY

IV. Appendix

APPENDIX A

Breach Notification – Definitions

1. Definition of "Breach." 45 CFR 164.402.

   a. A "Breach" is the acquisition, access, use or disclosure of protected health information ("PHI") in a manner not permitted by the HIPAA privacy rules.

   b. The following accidental workforce errors are not treated as Breaches:

      (1) An unintentional acquisition, access or use of protected health information by a member of the Plan Administration Staff or a member of a business associate's workforce if such acquisition, access or use was made in good faith and within the scope of the person's authority and does not result in further use or disclosure in a manner not permitted under the HIPAA privacy rules.

      (2) Any inadvertent disclosure by a member of the Plan Administration Staff or a member of a business associate's workforce to another member of the Plan Administration Staff or another member of the business associate's workforce and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA privacy rules.

      (3) A disclosure of PHI where the Plan or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

   c. An acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA privacy rules is not treated as a Breach if the Plan or business associate:

      (1) Conducts a risk assessment addressing at least the following factors:

         (a) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

         (b) The unauthorized person who used the protected health information or to whom the disclosure was made;

         (c) Whether the protected health information was actually acquired or viewed; and

(d) The extent to which the risk to the protected health information has been mitigated; and

(2) On the basis of the risk assessment, demonstrates that there is a low probability that the PHI was compromised.

2. Definition of "Secured." Only PHI that is Encrypted or destroyed is considered to be "Secured." 45 CFR 164.402.

a. Encrypted. Electronic PHI is "Secured" if it has been encrypted consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices. Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

b. Destroyed.

(1) Paper, film or other hard copy media PHI has been destroyed if it has been shredded or destroyed in such a way that the PHI cannot be read or otherwise cannot be reconstructed.

(2) ePHI has been destroyed if it has been cleared, purged or destroyed consistent with the NIST Special Publication 800–88, Guidelines for Media Sanitization such that the PHI cannot be retrieved.

APPENDIX B

FORMS

- Access Request Form
- Accounting Request Form
- Privacy Complaint Form
- Amendment Request Form
- Request for Confidential Communication
- Member Request to Restrict Uses and Disclosures of Personal Health Information (PHI)

Ohio University Health Plan

Access Request Form

You have the right of access to copy and/or inspect certain portions of your personal health information held by Ohio University Health Plan. We are not always required to grant such access but each request will be carefully reviewed and approved if warranted. You will be notified when your request has been approved or denied and the reasons for any denial. Access denial reasons can be found on the back of this form.

The following information is required to process your request:

Member/Dependent Information

Name_____ Date of Birth_____/_____/_____

Address_____ City_____

State and Zip _____

Phone_____ E-mail Address_____

Employee/Subscriber Information

Name_____ Employee ID_____

Requestor Information (complete if you are not the member)

Name _____

Address_____ City _____

State and Zip_____

Relationship to Member_____ Phone_____

Personal Health Information (PHI) you wish to review:

Organization

- ☐ The Ohio University Health Plan
- ☐ Medical
- ☐ Flexible Spending Account
- ☐ Vision Service Plan
- ☐ Global Care
- ☐ Dental

Information to Review

- ☐ Claims
- ☐ Enrollment
- ☐ Appeals
- ☐ Payment information

You have the option to receive the requested information in summary form with an explanation of what the information says in lieu of or in addition to the requested information.

- ☐ Yes, send me a summary/explanation *instead* of the complete information.
- ☐ Yes, send me a summary/explanation *in addition to* the complete information.
- ☐ No, send me the complete information only.

This form must be accompanied by signature page on the second page of this form.

Ohio University Health Plan

I wish to:

☐ Receive a copy of the information listed above by mail at the following address:
169 West Union Street, Athens, Ohio 45701
☐ Come in and inspect the information listed above at a mutually convenient time and place.
☐ Come in and pick up a copy of the information.
☐ Have the information sent to me via email (summary only).
☐ Other: _____

_____ _____
Signature **Date**

_____
Print Name

If you are a personal representative of a member, please provide documentation or explanation of your authority to act for the member.

Please note that we will not process any requests that are not signed by you or your personal representative.

Return this form to the HIPAA Privacy Officer, Ohio University Health Plan, 169 West Union Street, Athens, OH 45701 or fax to (740) 593-0386.

Denial of Access

We are permitted by law to deny part or all of your request for access for one or more of the following reasons:

- Your access request form is not signed by you or your representative;
- Your access request form is not signed by your representative and the representative has not provided information on the source of his/her authority to act for you;
- We do not maintain the information you have requested to copy or inspect;
- The information you have requested is not part of our records;
- Your request is for psychotherapy notes;
- Your request includes information complied for litigation;
- Your request includes information created or obtained in the course of research still in progress that includes your treatment and you agreed to this denial of access when consenting to participate in the research;
- A licensed health professional has determined that the requested access is likely to either endanger your or another person's life or safety or cause substantial harm to you or another person;
- Your request is to copy information and you are an inmate in a correctional facility (you retain the right to inspect the information);
- Your request relates to certain information that was obtained from a confidential source and we are not required to provide access to it by law.

FOR OFFICE USE:

APPROVED BY:_____ **DATE:**_____

Ohio University Health Plan

Accounting Request Form

You have the right to receive an accounting of any disclosures made by Ohio University Health Plan of your health and medical information. The following information is required to process your request:

Member Information

Name_____ Date of Birth_____/_____/_____

Address_____

Phone_____ E-mail Address_____

Employee/Subscriber Information

Name_____ Employee ID_____

Requestor Information (complete if you are not the member)

Name _____

Address_____

Relationship to Member_____ Phone_____

Organizations from which you wish to receive an accounting:

☐ Health Plan (Medical) ☐Vision Service Plan ☐Flexible Spending Account ☐ Dental
☐Other (please specify) _____

Period of time for which you wish to see the disclosures made _____

We are not required by law to include any of the following disclosures of your health information in an accounting to you:

- Disclosures made pursuant to an authorization signed by you or your representative;
- Disclosures to carry out our own or other providers' or plans' treatment, payment and health care operations;
- Disclosures made to you or to your personal representative;
- Disclosures made to persons involved in your care and/or payment or notification of next-of kin or family members;
- Disclosures for national security or intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials about inmates or others in custody; or
- Disclosures that occurred prior to six years from the date of this request.

_____ _____

Signature **Date**

Please note that we will not process any requests that are not signed by you or your personal representative.

Return this form to the HIPAA Privacy Officer, Ohio University Health Plan, 169 West Union Street, Athens, OH 45701 or fax to (740) 593-0386.

Ohio University Health Plan

Privacy Complaint Form

Ohio University Health Plan values the privacy of your personal health information. If you believe that anyone involved with the Ohio University Health Plan has inappropriately used or disclosed your personal health information, please let us know by completing this form. Ohio University Health Plan will review your complaint and all reasonable efforts will be made to resolve it.

Please provide enough information so complaint you are making may be understood (attach additional pages if necessary)

Are there documents available that provide additional information for review? If so, please provide information on the description and location.
May we contact you if additional information is needed? ☐ Yes (Please include contact information below) ☐ No

The following information is optional:

Name_____ Date of Birth_____

Mailing Address_____

E-mail Address_____ Phone Number_____

Employee ID_____

Please return this form and any supporting documentation to: HIPAA Privacy Officer, Ohio University Health Plan, 169 West Union Street, Athens, OH 45701 or fax to (740) 593-0386.

FOR OFFICE USE:

APPROVED BY:_____ **DATE:**_____

Ohio University Health Plan

Amendment Request Form

You have the right to request that Ohio University Health Plan make corrections or amendments to the personal health information we retain on your behalf if you believe something in that information is in error or needs to be amended. We are not always required to make the corrections or amendments you request, but each request will be carefully reviewed and corrections or amendments made if warranted. You will be notified when your request has been approved or denied.

Member/Dependent Information

Name_____ Date of Birth_____/_____/_____

Address_____ City_____

State and Zip_____

Phone_____ E-mail Address_____

Ohio University Employee/Subscriber Information

Name_____ Employee ID_____

Requestor Information (complete if you are not the member)

Name _____

Address_____ City_____

State and Zip_____

Relationship to Member_____ Phone_____

THIS SECTION MUST BE COMPLETED

Please provide as much detail as possible regarding the correction or amendment you seek in your personal health information. Be as specific as possible regarding the record type, the location, the date and the problem. For instance, "The request for pre-authorization of December 5, 2009 references a laboratory test from ABC laboratory for a blood test that I never received" or "Dr. Jones indicated in the records submitted with a claim on December 5, 2009 that I was suffering from weakness in my right leg when in fact the weakness is in my left leg." **To review the requested correction, we must be able to locate the record at issue and the exact entries or reports you want corrected.**

This form must be accompanied by signature page on the second page of this form.

Ohio University Health Plan

Please state precisely as possible how you would like to see the record worded.

If you are aware of anyone else (such as your physician, pharmacist, hospital, etc.) who also may have a copy of the record you seek to have corrected, please list those persons or organizations here with as much information as you have available regarding names and addresses.

I hereby authorize Ohio University Health Plan to notify person/entities I have listed above that may have a copy of the record I seek to have corrected and to provide them with the amended information.

_____ _____

Signature **Date**

_____

Print Name

If you are a personal representative of a member, please provide documentation or explanation of your authority to act for the member to the back of this form. Please note that we will not process any requests that are not signed by you or your personal representative.

Return this form to the HIPAA Privacy Officer, Ohio University Health Plan, 169 West Union Street, Athens, OH 45701 or fax to (740) 593-0386.

FOR OFFICE USE:

APPROVED BY:_____ **DATE:**_____

Ohio University Health Plan

Request for Confidential Communication

You have the right to request that we communicate with you on a confidential basis by requesting an alternative means or an alternative location to receive our communications. For instance, you may request that we send your Explanation of Benefits only to your work address. We will accommodate all reasonable requests for confidential communication. If you wish us to contact you at an address or phone number other than your home address or telephone, please provide us with the following information:

Member/Dependent Information

Name_____ Date of Birth_____/_____/_____

Address_____

Phone_____ E-mail Address_____

Employee/Subscriber Information

Name_____ Employee ID_____

Address to receive communications:

_____

_____

_____

Phone number to receive communications:

_____

Please describe in as much detail as possible any other alternative means you request we use in communication with you or any other alternative location not detailed above. You may use a separate sheet of paper, if necessary.

Do you believe that without this alternate communication, the disclosure of some or all of your information could endanger you? ☐ Yes ☐ No

_____ _____

Signature **Date**

_____

Print Name

If you are a personal representative of a member, please provide documentation or explanation of your authority to act for the member and attach to this form.
Please note that we will not process any requests that are not signed by you or your personal representative.

FOR OFFICE USE:

APPROVED BY:_____ **DATE:**_____

Return this form to the HIPAA Privacy Officer, Ohio University Health Plan, 169 West Union Street, Athens, OH 45701 or fax to (740) 593-0386.

Ohio University Health Plan

Member Request to Restrict Uses and Disclosures of Personal Health Information (PHI)

Member/Dependent Information

Name_____

Date of Birth_____/_____/_____ Address _____

City_____ State and Zip_____

Phone_____ E-mail Address_____

Employee/Subscriber Information

Name_____

Employee ID_____

Requestor Information (complete if you are not the member)

Name _____

Address_____ City_____

State & Zip_____ Phone_____

Relationship to Member_____

THIS SECTION MUST BE COMPLETED

I hereby request that the following restriction(s) be placed on the uses and disclosures of my personal health information by the Ohio University Health Plan.

Benefits affected: ☐ Medical ☐ Vision ☐ Flexible Spending Account ☐ Dental

List of Restrictions Requested

Please give a full, specific description of the type of restrictions you are requesting regarding how and to whom your personal health information is used and disclosed. Restrictions may only be requested for those uses and disclosures that relate to your treatment, your payment or insurance, or the business operations of Ohio University Health Plan. (For example, you may request that we restrict the use of your information for disease management purposes.)

Ohio University Health Plan

I understand that Ohio University Health Plan is not required to agree to my restriction requests, but that Ohio University Health Plan may only be required to attempt to accommodate reasonable requests when appropriate. I further understand that Ohio University Health Plan reserves the right to terminate an agreed-to restriction if it feels that termination is appropriate, and that I also have the right to terminate, in writing, any restriction by sending a termination notice to the Privacy Officer at the address at the bottom of this form.

_____ _____

Signature **Date**

_____

Print Name

Return this form to the HIPAA Privacy Officer, Ohio University Health Plan, 169 West Union Street, Athens, OH 45701 or fax to (740) 593-0386.

FOR OFFICE USE:

APPROVED BY:_____ **DATE:**_____