UNIVERSITY OF CENTRAL ARKANSAS

HIPAA PRIVACY POLICY

Table of Contents

I. PURPOSE

A. The University of Central Arkansas adopts this policy to establish requirements for the use and disclosure of individually identifiable protected health information in conformance with the Health Insurance Portability and Accountability Act of 1996, and the Health Information Technology for Economic and Clinical Health Act of 2009.

B. This policy does not apply to health information contained within education records covered under the Family Educational Rights and Privacy Act ("FERPA").

II. WHO IS SUBJECT TO THIS POLICY

A. The University of Central Arkansas is a Hybrid Entity because certain University employees provide Treatment in a University created clinic or faculty practice and submit medical bills to federal or state reimbursement programs or private health insurance carriers for Payment. The Health Care Components of the University are listed in Exhibit A and must comply with this Policy.

III. DEFINITIONS

The following definitions shall apply to the following terms throughout this Policy and without regard to whether they are capitalized. All undefined terms shall have the same meaning as defined by HIPAA.

Accounting of Disclosures – A written record of certain disclosures of PHI that may be required to be maintained and provided to a requesting individual under certain circumstances described in this policy.

Access – the ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any system resource.

Authorization – A written document completed and signed by the individual that generally allows use and disclosure of PHI for purposes other than Treatment, payment or health care operations.

Breach - the acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA which compromises the security or privacy of the PHI. Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a Workforce member or person acting under the authority of a Healthcare Component or Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by HIPAA.

(ii) Any inadvertent disclosure by a person who is authorized to access PHI at a Healthcare Component or Business Associate to another person authorized to access PHI at the same Healthcare Component or Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

(iii) A disclosure of PHI where a Healthcare Component 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.

Business Associate. An entity, other than in the capacity of a member of the Healthcare Component workforce, that creates, receives, maintains, or transmits PHI for on behalf of Healthcare Component or that provides services to or for Healthcare Component where the provision of services involves the disclosure of Healthcare Component's PHI. 45 C.F.R. § 160.103.

Covered Entity – the Health Care Components designated by UCA.

Covered Function – Those functions of a Healthcare Component the performance of which makes the Healthcare Component subject to HIPAA.

De-identified Information – 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. De-identified Information is not subject to the HIPAA Privacy Rule.

Designated Record Set – Medical or billing records about individuals maintained by or for a healthcare provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or records used in whole or in part by or for the provider to make decisions about individuals.

Discovery of a Breach. A Breach is considered to be discovered by Healthcare Component as of the first day on which the Breach is known to Healthcare Component or should have been known to Healthcare Component if it had exercised reasonable due diligence.

Disclosure – the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Health care – Care, services, or supplies related to the health of an individual. Health Care includes, but is not limited to, the following: Preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service assessment, or procedure with respect to the physical or mental condition, or functional status, or an individual or that affects the structure or function of the body; and Sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Health Care Component – A component of the University in accordance with its designation as a hybrid entity as listed in Exhibit A.

Health Information – Any information, whether oral or recorded in any form or medium, that:

1. is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

2. relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

HIPAA – Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d *et seq.*

HIPAA Privacy Regulations – The HIPAA Standards for Privacy of Individually Identifiable Health Information, as set forth in 45 CFR Parts 160 and 164 and as otherwise amended.

Individually Identifiable Health Information – information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Privacy Officer shall mean the individual appointed by the President to assume the obligations of the Privacy Officer in this Policy.

Protected Health Information ("PHI") - Protected health information means individually identifiable health information that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual, and identifies or could reasonably be used to identify the individual.

PHI includes information that is transmitted by electronic media; maintained in electronic media or transmitted or maintained in any other form or medium.

PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USC 1232g; records described at 20 USC 1232g(a)(4)(B)(iv); and employment records[1] held by a Healthcare Component in its role as employer.

Payment - activities undertaken by a Healthcare Component to obtain payment for the provision of healthcare; and relates to the individual to whom health care is provided.

Personal Information ("PI") – an individual's first name or first initial and last name linked with one or more of the following data elements:

[1] Employment records that are not subject to this HIPAA Privacy Policy include medical information needed to carry out the University's obligations under the Family Medical Leave Act, the American's with Disabilities Act, and similar laws, as well as files or records related to occupational injury, disability insurance eligibility, sick leave requests and justifications, drug screening results, workplace medical surveillance, and fitness-for-duty tests of employees.

1. Social Security number

2. Driver's license number or State identification card number

3. account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Personally Identifiable Information ("PII") – Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Protected Health Information ("PHI") - Any oral, written, or electronic individually identifiable health information maintained or transmitted in any form or medium. Individually identifiable health information includes demographic information and any information that relates to past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to any individual.

Psychotherapy notes – Notes recorded (in any medium) by a health care provider who is a mental health professional that:

1. Document or analyze the contents of conversation during a private counseling session or a group, joint or family counseling session, and

2. Are separated from the rest of the individual's medical record.

3. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of Treatment furnished, results of clinical tests, and any summary diagnosis, functional status, Treatment plan, symptoms, prognosis, and progress to date.

Psychotherapy notes are used only by the therapist who wrote them, maintained separately from the medical record and not normally involved in the documentation necessary for health care Treatment, payment or health care operations.

Public health authority – An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

Treatment – the provision, coordination, or management of health care and related services by one or more health care providers, including:

1. the coordination or management of health care by a health care provider with a third party

2. consultation between health care providers relating to a patient, or

3. the referral of a patient for health care from one health care provider to another.

"TPO" – To carry out treatment, payment or healthcare operations

UCA – University of Central Arkansas.

University – University of Central Arkansas

Unsecured PHI. Protected health information that is not encrypted and rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the Department of Health and Human Services (HHS).

Workforce – employees, volunteers, trainees, and other persons whose conduct, in the performance of work is under the direct control of the Healthcare Component, whether or not their services are paid by the entity.

IV. HYBRID ENTITY DESIGNATION

A. The University has designated itself a Hybrid Entity in accordance with HIPAA and adopts this Policy to ensure that its Health Care Components comply with the requirements of HIPAA.

1. The University's Health Care Components are listed in Exhibit A. Exhibit A shall be retained for at least six (6) years following any decision to terminate any division or department from the University's Health Care Components. Designations that remain a Health Care Component of the University should be retained permanently.

2. Security procedures must be implemented between Health Care Component's Covered Functions and all other functions. Specifically, UCA will ensure that:

a. In circumstances that require a Health Care Component to disclose PHI to any department, division, school or college that is not a Health Care Component, the Health Care Component shall clearly mark the PHI as confidential;

b. Each department, division, school or college within UCA that receives PHI shall not use or disclose PHI that it creates or receives from or on behalf of the Health Care Component in a way that is prohibited by HIPAA Privacy Regulations and Privacy Rule, and otherwise complies with HIPAA's Security Standards.

c. Wherever possible, UCA Workforce performing Covered Functions shall be separated from Workforce that is performing other functions.

d. If a Workforce member performs duties for both a Health Care Component and other department, division, School or College that is not a Health Care Component, such Workforce member must not use or disclose PHI created or received in the course of or incident to the Workforce member's work for the Health Care Component in a way prohibited by this Policy.

V. USE AND DISCLOSURE OF PHI WITH AND WITHOUT CONSENT

A. Healthcare Component shall protect PHI from disclosure as required by this Policy.

B. Healthcare Component may not use or disclose PHI without a signed authorization by the individual from whom the PHI was created unless it is otherwise permitted under HIPAA, including under the following circumstances:

1. When requested by the Secretary of the United States Department of Health and Human Services ("DHHS") to investigate or determine compliance with privacy standards;

2. When the disclosure is to the individual to whom the PHI pertains, or a legal personal representative, including requests for accounting or access to inspect or copy;

3. To carry out treatment, payment or healthcare operations (hereinafter collectively referred to as "TPO");

4. Where an opportunity to agree or to object has been afforded to the individual and the individual does not object to the use and disclosure of PHI in the following circumstances:

a. To family and friends involved with the individual's care or payment related to the individual's healthcare, or

b. To disaster relief agencies to coordinate the notification of family and friends regarding the individual's location, condition, or death;

d. For information needed by coroners, medical examiners and funeral directors.

e. For information needed to facilitate an organ donation.

f. To alert a law enforcement agency of the death if the Healthcare Component has a suspicion that such death may have resulted from criminal conduct. If the agency is already investigating the death, other law enforcement powers to obtain PHI may apply.

5. When the information listed in Exhibit B has been de-identified and there is no actual knowledge by the Healthcare Component that any of the remaining information could identify the individual.

6. As otherwise permitted under the HIPAA regulations.

C. In the event any state and federal law affords protection to privacy rights greater than this Policy, Healthcare Component shall comply with such greater obligations, (e.g. treatment for drug and alcohol use, HIV/AIDS, and mental health).

1. For psychotherapy notes, a valid authorization must be obtained for any use and disclosure unless otherwise permitted by HIPAA.

D. Uses and Disclosures for TPO

1. Healthcare Component may use and disclose PHI necessary to provide Treatment, obtain Payment, and conduct administrative and operational tasks as necessary to provide Health Care Services in accordance with Exhibit C.

2. Patients may request restrictions on the uses or disclosures of PHI for TPO. Healthcare Components must restrict disclosure of PHI if: a) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and b) the PHI pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the Healthcare Component in full.

3. The following types of activities require a written authorization from the individual who generates the PHI:

a. Marketing and fundraising activities require an authorization prior to the use and disclosure and PHI. The University will comply with HIPAA in the event it uses PHI for marketing purposes. All Workforce shall consult the Privacy Officer and University Counsel before using any PHI for marketing in order to ensure compliance with HIPAA.

b. Research activities require a written authorization unless there is written documentation that the University's IRB either waived or altered the requirement. See Exhibit C for requirements and specifications under which an authorization would not be required for Research.

E. Opportunity to Agree or Object

In the following three (3) circumstances, PHI may be disclosed without an authorization as long as the patient is given an opportunity to agree or object. Healthcare Component must establish a process to document that opportunity was afforded and if the individual objected.

1. To Persons involved in Treatment or Payment

a. PHI may be disclosed to a family member, a personal representative of the individual or another person when:

i. That information is relevant to such person's involvement with the individual's care or payment related to such care, or

ii. To notify (or assist in the notification of) such persons of the individual's location, general condition or death, and

iii. When sections below are complied with.

b. If the individual is present and has the capacity to make healthcare decisions, the Healthcare Component may use or disclose the PHI only if it:

i. Obtains the individual's agreement;

ii. Provides the individual the opportunity to object and the individual does not object; or

iii. Can be reasonably inferred from the circumstances, using its professional judgment, that the individual does not object to the disclosure.

c. If the individual is incapacitated or unable to consent due to emergency circumstance, the PHI may be disclosed only if:

i. The PHI is directly relevant to the person's Treatment, and it is in the individual's best interest:

ii. Healthcare Component may use professional judgment and experience with common practice to make reasonable inferences regarding the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-ray films, or other similar forms of PHI.

2. Disaster Relief Efforts

PHI may be used or disclosed to a public or private entity to assist in disaster relief efforts. The above rules for use and disclosure of PHI for involvement in an individual's Treatment and notification (depending upon whether the individual is present or not) apply as long as they do not interfere with the ability to respond to a disaster relief situation.

F. Authorizations

1. UCA shall maintain an authorization form that complies with HIPAA. A sample authorization is attached as Exhibit D.

G. Extent of the Information That May be Used and Disclosed.

1. The University may disclose only the information specified in a validly executed authorization.

2. In the absence of a validly executed authorization, the University must make reasonable effort to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary rule does not apply to the following circumstances:

    a. Disclosures to or requests by a health care provider for Treatment;

    b. Disclosures to the individual or personal legal representative who is the subject of the PHI;

    c. Uses or disclosures required for compliance with electronic transactions;

    d. Disclosures to the DHHS when disclosure of information is required under HIPAA or this Policy for enforcement purposes; and

    e. Uses and disclosures that are required by any other law.

3. Healthcare Component will use reasonable efforts to limit the disclosure of PHI to the minimum necessary to accomplish the intended purpose. A disclosure shall be the minimum necessary for a stated purpose when:

    a. Healthcare Component is making disclosures to a public official where no authorization or consent is required, and the public official represents that the information requested is the minimum necessary;

    b. The information is requested by another health care provider, health plan or health care clearing house covered under HIPAA;

    c. The information is requested by a professional who is a member of UCA's Workforce or a Business Associate for the purpose of providing professional services to Healthcare Component, if the professional represents that the information requested is the minimum necessary for the stated purpose; or

    d. Documentation or representations are made that comply with the uses and disclosures involving research in accordance with HIPAA.

H. Verification Requirement

1. Each member of the Workforce will verify as applicable and in accordance with HIPAA the identity and authority of persons requesting PHI.

2. If the requesting person is a public official or someone acting on his or her behalf, the Healthcare Component may rely upon the following:

a. Agency identification badge, credentials or other proof of status;

b. Government letterhead, if request is made by letter;

c. A written statement of the legal authority (or, if impracticable, an oral statement) under which the information is requested.

d. If a request is made pursuant to a legal process, warrant, subpoena, order, or other legal process, it is presumed to constitute legal authority.

e. For persons acting on behalf of the official, a written statement on government letterhead or other evidence or documentation that establishes that the person is acting under the public official's authority (such as contract for services, memo of understanding).

f. In the event a request for disclosure is provided by a public official, the University's Workforce should forward all such requests to the Office of General Counsel for review and response.

3. Healthcare Component may rely on the exercise of professional judgment as to disclosures pursuant to persons involved in a patient's Treatment or Payment, and in relation to disaster relief as discussed in this Policy. As to disclosures regarding serious threats to health and safety, Healthcare Component shall exercise its judgment in accordance with Exhibit C.

VI. APPOINTMENT OF PRIVACY OFFICER

A. The President or his designee shall appoint a Privacy

Officer. B. The Privacy Officer is responsible for:

1. Maintaining the master copy of the Notice of privacy; and

2. In consultation with General Counsel, approving requested changes to the Notice by Healthcare Component.

3. Receiving questions and complaints regarding the Notice;

4. Coordinating the investigation of a Breach and any associated notice related to such Breach;

5. Reviewing and responding to requests for Limited Data Sets;

6. Evaluating Business Associate Agreements; and

7. Receiving notice of a Breach of a Business Associate Agreement, coordinating the investigation of such Breach, and coordinating any associated notice related to such Breach.

C. The Privacy Officer must document compliance with the Notice requirements of this policy by retaining copies of the original and any subsequent revisions of the Notice issued by the Healthcare Component for six years from the date of the creation of the Notice, or the date when it last was in effect, whichever is later.

VII. NOTICE OF PRIVACY

A. A form of Notice of Privacy Practices is attached as Exhibit E to this Policy and must be posted on the webpages for the Healthcare Components within the University's website.

B. Revisions to Notice of Privacy Practices:

1. Healthcare Component must , in accordance with HIPAA, revise and distribute its Notice in accordance with HIPAA whenever there is a material change to the uses or disclosures, the individual's rights, the Healthcare Component's legal duties, or other privacy practices stated in the Notice.

2. Except when required by law, a material change to any term of the Notice may not be implemented prior to the effective date of the Notice in which the change is reflected.

3. Whenever the Notice is revised, Healthcare Component shall make the revised Notice available to patients upon request on or after the effective date of the revision and must post the Notice on their webpage, if any, and in clear and prominent locations within each Healthcare Component.

C. Face-to-Face Provision of the Notice of Privacy Practices:

1. The Notice must be offered to all individuals whenever they enter a Healthcare Component seeking health care services or otherwise receive health care services from UCA.

2. Healthcare Component must provide the Notice to individuals at the first provision of services.

   a. In emergency situations, Healthcare Component must provide the Notice as soon as reasonably practicable after the emergency situation is resolved. At the time the Notice is provided, Workforce members may offer to answer questions regarding the Notice.

3. Except in an emergency situation, upon provision of the Notice, Workforce members must make a good faith attempt to obtain a written acknowledgement of receipt of the Notice signed by the patient and his/her personal representative. If the acknowledgement cannot be obtained, staff must document their efforts to obtain acknowledgement and the reason the acknowledgement was not obtained.

4. If the Notice cannot be provided and/or the acknowledgement is not signed due to an emergency situation, Workforce members must provide the Notice and attempt

to obtain the acknowledgement as soon as reasonably practical after the emergency treatment situation is resolved.

5. A copy of the Notice must be posted in prominent locations at each Healthcare Component.

D. Provision of Notice of Privacy Practices in Special Circumstances:

1. *By Telephone* – In the event the initial delivery of health care services occurs over the telephone, the Notice must be mailed to the patient no later than the next day or be emailed to the patient (see "*By E-Mail,*" below). The clinic must include an acknowledgement and request the patient to sign the acknowledgement and mail or otherwise return it to the Healthcare Component. The clinic must document that the patient was instructed to sign and return the acknowledgement to the clinic. Attached to this Policy as Exhibit F is a sample acknowledgement to be used when mailing the Notice to the patient.

2. *By E-Mail* – If the initial delivery of health care series occurs electronically, the Healthcare Component must automatically provide electronic Notice to the patient. Notice may be sent to the patient by e-mail if the patient agrees to receive the Notice electronically and such agreement has not been withdrawn. When the Notice is sent by e-mail, the Healthcare Component must include a standard message asking the recipient to return an e-mail acknowledgement that he or she has received the Notice.

   a. If the Healthcare Component's staff knows that the e-mail transmission failed, a paper copy of the Notice must be given to the patient upon first delivery of service.

   b. Any patient who is a recipient of an electronic Notice retains the right to obtain a paper copy of the Notice upon request.

E. Dissemination of Notice

1. Workforce members in the Healthcare Component are responsible for providing the Notice to patients, answering questions, and collecting the acknowledgement.

2. The Healthcare Component is responsible for maintaining copies of written acknowledgements of receipt of the Notice or documentation of good faith efforts to obtain such written acknowledgement for six years from the date of creation.

VIII. ACCESS BY INDIVIDUALS TO PHI

Healthcare Component must provide an individual with the right of access to inspect and obtain a copy of PHI pertaining to the individual in a designated record set as long as the record is maintained. Individuals shall make requests for such access in writing.

A. Requirements:

1. Healthcare Component shall provide individuals an opportunity inspect and copy their PHI, unless an exception applies, including but not limited to:

   a. psychotherapy notes; and

   b. information complied in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding

2. Healthcare Component may deny an individual access if the individual has given a right to have such denial reviewed by the Privacy Officer and the following circumstances are present:

   a. The access requested is reasonably likely to endanger the life or physical safety of the individual or another person.

   b. The PHI makes reference to another person and the access requested is reasonably likely to cause substantial harm to such other person.

   c. The request for access is made by the individual's personal representative and access is reasonably likely to cause substantial harm to the individual or another person.

B. Responsibilities:

1. If an individual has been denied access to records and has requested a review of a denial, the Healthcare Component in possession of the records shall, in accordance with HIPAA, designate, and refer the request to the Privacy Officer to review the decision to deny access. The Privacy Officer, within a reasonable period of time but not to exceed 90 days, must determine whether or not to deny access based on the standards put forth in this Policy. Privacy Officer shall, in accordance with HIPAA, provide written notice to the requesting individual of the determination and take other actions as required to carry out the determination.

2. Healthcare Component must act on requests to access PHI within thirty (30) days after receipt of a request. If the request is for PHI not maintained or accessible to the Healthcare Component, the Healthcare Component may take action by no later than sixty (60) days from the receipt of such a request. However, the Healthcare Component must provide a written statement of the reasons for the delay and the date by which it will complete its action on the request. No other time extensions will be granted in excess of sixty (60) days.

3. If the Healthcare Component grants the request to access the PHI, in whole or in part, it shall inform the individual of the acceptance of the request and:

   a. Provide the access requested.

      Healthcare Component must allow inspection or provide a copy or both, of the PHI in designated record sets. If the same PHI that is the subject of a

request for access is maintained in more than one designated record set or at more than one location, Healthcare Component shall only produce the PHI once in response to a request for access.

b. Provide access in the form requested.

i. Healthcare Component shall provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or in a readable hard copy form or such other form or format as agreed to by Healthcare Component and the individual.

ii. Notwithstanding the preceding paragraph, if the PHI that is the subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, the Healthcare Component must provide the individual with access to the PHI in the electronic form and format requested by the individual if it is readily producible in such form and format; or, if not, in a readable electronic form and format, then as agreed to by the Healthcare Component and individual.

iii. Healthcare Component may provide the individual with a summary of the PHI requested, instead of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if: (x) The individual agrees in advance to such a summary or explanation; and (y) The individual agrees in advance to the fees imposed, if any, by the Healthcare Component for such summary or explanation.

c. Manner of Access

i. Healthcare Component must provide access, by arranging with the individual a convenient time and place, to inspect or obtain a copy of the PHI; or mail a copy of the PHI at the individual's request. Healthcare Component may discuss the scope, format, and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

ii. If an individual's request for access directs the Healthcare Component to transmit the copy of PHI directly to another person designated by the individual, the Healthcare Component must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual and clearly identify the designated person and where to send the copy of PHI.

iii. If the individual requests a copy of the PHI or agrees to a summary or explanation of information, Healthcare Component may impose a reasonable cost-based fee, provided that the fee includes only the cost of: (a) labor for copying the PHI requested whether in paper or electronic form; (b) supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; (c) postage, when the individual has requested the copy or explanation be mailed; and (d) preparing an explanation or summary of the PHI, if agreed to by the individual as required by HIPAA.

d. If Healthcare Component denies the request to access the PHI, in whole or in part, it must provide the individual with a timely written denial. The denial must be in plain language and contain:

i. The basis for the denial.

ii. A statement of the individual's review rights, including a description of how the individual may exercise such review rights.

iii. A description of how the individual may complain to Privacy Officer or the Department of Health and Human Services (DHHS), pursuant to this Policy's procedures. The description must include the name, or title, and telephone number of the contact person or office.

e. If Healthcare Component does not maintain the PHI that is the subject of the individual's request for access, and Healthcare Component knows where the requested information is maintained, Healthcare Component must inform the individual where to direct the request for access.

f. Healthcare Component must document and retain the following information:

i. The designated record sets that are subject to access by individuals.

ii. The titles of the persons or offices responsible for receiving and processing requests for access by individuals.

g. All requests made for access to PHI must be made to the individual designated by the Healthcare Component to receive such requests.

IX. REQUESTS FOR RESTRICTION OF USE AND DISCLOSURE OF PHI

A. Requirements:

1. Individuals shall be permitted to request that Healthcare Component restrict:

a. uses and disclosures of PHI to carry out TPO; and

b. disclosures related to involvement in Treatment.

2. Healthcare Component may, however, deny the request.

3. All requests for restrictions and termination of the agreement to restrict must be in writing.

4. All requests made for restrictions to PHI must be made to the individual designated by the Healthcare Component within the Health Care Component to receive such requests.

B. Responsibilities:

1. A Healthcare Component must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from the Healthcare Component by alternative means or at alternative locations. Healthcare Component must review all requests that are made by individuals to restrict use and disclosure of the individuals PHI; however, it shall not be required to agree to the restrictions requested if it determines that the restrictions would interfere with Treatment, Payment or Health Care Operations. If restricted PHI is disclosed to a health care provider for emergency treatment, the Healthcare Component must request that such health care provider not further use or disclose the information.

2. If Healthcare Component agrees to an individual's restriction request, the restriction must be appropriately documented and such documentation be retained by the Healthcare Component. Also, the restriction must be communicated in a manner as to assure that anyone accessing the information becomes aware of the restriction.

3. If the Healthcare Component agrees to an individual's restriction request, it is not permitted to use or disclose the specified PHI in any manner that would not violate that restriction, except in the event that the individual is in need for emergency Treatment and the restricted PHI is needed to provide such Treatment. In this case, Healthcare Component may use the restricted PHI or disclose the PHI to a Healthcare Provider to provide such Treatment to the individual. In this event, Healthcare Component must request that such provider not further use or disclose the information.

4. Healthcare Component may terminate a restriction if:

a. the individual agrees to or requested the termination in writing;

b. the individual orally agrees to the termination and the oral agreement is documented; or

c. Healthcare Component informs the individual that it is terminating its agreement to restriction.

5. In the event that Healthcare Component, for any of the above mentioned reasons, terminates the agreement for restriction, the termination is only effective with respect to PHI created or received after it has so informed the individual.

X. REQUESTS FOR AMENDMENT OF PHI

A. Healthcare Component shall maintain a process to enable its patients to request an amendment of their Individual Health Information held by the Healthcare Component by designating a person within the Healthcare Component to receive such requests. Such requests must be made in writing and include a reason supporting the amendment.

1. An individual may request the Healthcare Component amend his or her Individual Health Information. Individuals shall make such requests in writing and provide a reason to support the amendment. The Health Healthcare Component shall provide all individuals Notice of the University's Privacy Practices prior to Treatment.

2. The Healthcare Component may deny the request to amend if the Individual Health Information that is the subject of the request meets the following conditions:

   a. It was not created by the Healthcare Component, unless the originator is no longer available to act on the request.

   b. It is not part of the individual's Designated Health Record.

   c. It would not be accessible to the individual pursuant to this Policy's section entitled Access of Individual's Protected Health Information.

   d. It is accurate and complete.

3. Healthcare Component must act on the individual's request for amendment no later than sixty (60) days after receipt of the request for an amendment. Healthcare Component may extend the time to respond no more than thirty (30) days provided the Healthcare Component gives the individual a written statement of the reason for the delay, and the date by which the amendment will be processed.

4. If the request is granted, Healthcare Component shall:

   a. Insert the amendment or provide a link to the amendment at the site of the information that is the subject of the request for amendment.

   b. Inform the individual that the amendment is accepted.

Healthcare Component

c. Within a reasonable time frame, make reasonable efforts to provide the amendment to persons identified by the individual, and persons, including business associates, that the Healthcare Component knows have the PHI that is the subject of the amendment and that may have relied on or could foreseeably rely on the information to the detriment of the individual.

5. If the Healthcare Component denies the request for amendment, it must provide the individual with a timely, written denial in plain language that states:

   a. The basis for the denial.

   b. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement.

   c. A statement that if the individual does not submit a statement of disagreement, the individual may request the Healthcare Component to provide the individual's request for amendment and the denial with any future disclosures of PHI.

   d. A description of how the individual may complain to the Privacy Officer designated by the Healthcare Component or to the Secretary of DHHS.

6. The individual requesting the amendment shall submit to the Healthcare Component a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The University may reasonably limit the length of a statement of disagreement.

7. Healthcare Component may submit a rebuttal to the individual's statement of disagreement, and provide a copy to the individual who submitted the statement of disagreement.

8. Healthcare Component shall, as appropriate, identify the record of PHI that is the subject of the disputed amendment, append the individual's request for an amendment, the denial of the request, the individual's statement of disagreement, if any, and the rebuttal, if any.

9. If the individual has not submitted a written statement of disagreement, Healthcare Component must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of PHI only if the individual has requested such action.

10. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included, Healthcare Component may separately transmit the material required.

11. Healthcare Component that is informed by another Healthcare Component of an amendment to an individual's PHI must amend the PHI in written or electronic form.

12. Healthcare Component shall document the titles of the positions responsible to receive and process requests for amendments.

XI. BREACH NOTIFICATION

A. **General**. Healthcare Component will presume that any acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted under the HIPAA Privacy Rule is a Breach that requires notification to affected individuals or to their personal representatives, unless an exception applies or Healthcare Component demonstrates that there is a low probability that the Unsecured PHI has been compromised, based on a risk assessment (described below). Upon Discovery of a Breach, Healthcare Component may, at its discretion, either (1) notify affected individuals or their personal representatives of the Breach without conducting a risk assessment, or (2) first conduct a risk assessment to determine if such notification is necessary. All Business Associates of Healthcare Component are required to report any Breach to Healthcare Component without unreasonable delay upon discovery and in no case later than 60 calendar days after discovery.

1. If Healthcare Component discovers a potential Breach of Unsecured PHI and chooses to provide automatic notification or conducts a risk assessment and determines there is more than a low probability that the Unsecured PHI has been compromised, Healthcare Component must notify affected individuals or their personal representatives of the Breach without unreasonable delay and in no case later than 60 days of Discovery of a Breach. A Breach is considered discovered as of the first day on which the Breach is known by any workforce member or agent of Healthcare Component, or, in the exercise of reasonable diligence, would have been known to any person, other than the person committing the Breach, who is a workforce member or agent of Healthcare Component.

B. **Internal Reporting**. Any member of the Healthcare Component workforce must promptly notify his or her supervisor(s) and/or the Healthcare Component of any unauthorized access, use, or disclosure of Unsecured PHI, provide relevant facts regarding the unauthorized incident, and cooperate with any subsequent investigation.

1. **Incident Response**. The Privacy Officer will work with the appropriate Healthcare Component officials and General Counsel, as necessary, to determine an appropriate and timely response to the incident.

2. **Workforce Training**. All appropriate members of the Healthcare Component workforce will be trained how to identify and report potential Breaches and will be trained on any other applicable policies and procedures

related to PHI that are appropriate with respect to the member's job function. Appropriate sanctions, up to and including termination, will be applied against members of the workforce who fail to comply with this policy.

C. **Investigation**. The Privacy Officer will work with the appropriate workforce members, Healthcare Component officials, and General Counsel, as necessary, to uncover the facts and circumstances related to the incident. The investigative actions may include, but will not be limited to, conducting employee interviews, system audits, and site observation. Upon completion of the investigation, if Healthcare Component determines that the incident is an impermissible acquisition, access, use, or disclosure of Unsecured PHI, Healthcare Component will presume the incident is a Breach and will:

1. **Notify/Assess**. Provide notification as set forth below upon conferring with Healthcare Component officials and General Counsel, as necessary, to determine the financial and reputational costs to Healthcare Component; **or** conduct a risk assessment, as set forth below, to determine if there is a low probability that the Unsecured PHI has been compromised. Healthcare Component is not required to provide notification if it demonstrates a low probability of compromise upon completion of the risk assessment.

2. **Mitigate Harm**. Mitigate, to the extent practicable, any harmful effects of the Breach that are known.

3. **Delay if Required by Law Enforcement**. Healthcare Component will delay notification if a law enforcement official states that such notification would impede a criminal investigation or would cause damage to national security. Healthcare Component will delay the notification as specified in a written statement from law enforcement or, if no written statement is provided, for not more than 30 days from the date Healthcare Component is in receipt of oral notification from law enforcement. Healthcare Component will document any such oral communication in writing.

D. **Risk Assessment**. If Healthcare Component chooses not to provide default notification upon Discovery of a Breach, then it must conduct a risk assessment of any acquisition, access, use, or disclosure of Unsecured PHI in a manner not permitted by the HIPAA Privacy Rule to determine whether there is a low probability that the impermissible acquisition, access, use, or disclosure compromised the security or privacy of the Unsecured PHI. The risk assessment will take into account the factors listed below to determine whether there is a low probability that Unsecured PHI has been compromised. The factors indicated below do not necessarily constitute an exhaustive list of items that Healthcare Component will consider to determine if there exists a low probability of compromise of Unsecured PHI. Circumstances involving a Breach will be analyzed on a case-by-

case basis and may require consideration of factors in addition to those included in the following:

1. **Nature of the Data Elements Breached**. Healthcare Component will analyze the nature of the data elements compromised in the impermissible acquisition, access, use, or disclosure. The nature of the data elements involved is a key factor to consider in determining if a Breach has occurred that requires notification. It is difficult to characterize data elements as creating a low, moderate, or high risk simply on the basis of the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context. In assessing the levels of risk and harm, Healthcare Component will consider the data element(s) in light of their contexts, including the types of identifiers in the data element(s), the likelihood of re-identification of the information, and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

2. **The Unauthorized Person Who Used the Unsecured PHI or to Whom the Disclosure Was Made**. Healthcare Component will consider who impermissibly used the Unsecured PHI or to whom a disclosure was made. If the person in receipt of the Unsecured PHI has an obligation to protect PHI (e.g., another covered entity governed by HIPAA), that fact will weigh in favor of a finding of low probability that the Unsecured PHI is compromised.

3. **Likelihood the Unsecured PHI Was Actually Acquired or Viewed**. Healthcare Component will assess the likelihood that Unsecured PHI will be or had been acquired or used by unauthorized individuals. The fact that Unsecured PHI is lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. The number of physical, technical, and procedural safeguards utilized by Healthcare Component impact the risk that the information is accessible or useable.

4. **Extent to Which the Risk to the Unsecured PHI Has Been Mitigated**. The probability that Unsecured PHI has been compromised may depend, in part, upon whether, and to what extent, Healthcare Component has mitigated the effects of an impermissible use or disclosure. Appropriate countermeasures, such as monitoring of systems for use of personal information and patterns of suspicious behavior, will be taken by Healthcare Component. In assessing risk, Healthcare Component will consider, among other factors, whether the Unsecured PHI has been returned, remotely wiped, or destroyed, and whether the unauthorized recipient of the Unsecured PHI has provided satisfactory assurances that the Unsecured PHI will not be further used or disclosed.

5. The burden to determine whether there is a low probability that Unsecured PHI has been compromised belongs to Healthcare Component. In order to

make this determination, Healthcare Component will document each impermissible acquisition, access, use, and disclosure and the risk assessment outlined above will be conducted for each, except in the event that Healthcare Component elects to provide automatic notification. The Privacy Officer will be responsible for conducting the risk assessment, documenting the results of the assessment, and determining whether there exists a low probability that the Unsecured PHI has been compromised.

E. **Notification**

1. Individual Notification

a. If Healthcare Component elects to provide automatic notification, or if the risk assessment determines that a Breach has occurred and more than a low probability that the Unsecured PHI has been compromised exists, then without unreasonable delay and in no case later than 60 days from the Discovery of a Breach, Healthcare Component will provide written notice to the affected individual or:

i. If the individual is deceased, to the next of kin or personal representative.

ii. If the individual is incapacitated/incompetent, to the personal representative.

iii. If the individual is a minor, to the parent or guardian.

b. Written notification will be in plain language.

c. Written notification will be sent to the last known address of the affected individual or next of kin by first-class mail, or if specified by the affected individual, by encrypted electronic mail.

d. Written notification will contain the following information:

i. A brief description of what occurred with respect to the Breach, including, to the extent known, the date of the Breach and the date on which the Breach was discovered;

ii. A description of the types of Unsecured PHI that were disclosed during the Breach;

iii. A description of the steps the affected individual should take in order to protect himself or herself from potential harm caused by the Breach;

iv. A description of what Healthcare Component is doing to investigate and mitigate the Breach and to prevent future Breaches; and

v. Instructions for the individual to contact Healthcare Component.

e. In the case where there is insufficient or out-of-date contact information:

i. For less than ten (10) individuals, a substitute form of notice shall be provided, such as a telephone call.

ii. In the case that there are ten (10) or more individuals for which there is insufficient or out-of-date contact information and contact information is not obtained, Healthcare Component will:

(a) Post a conspicuous notice for 90 days on the homepage of its website that includes a toll-free number; or

(b) Provide notice in major print or broadcast media in the geographic area where an affected individual can learn whether or not his or her Unsecured PHI is possibly included in the Breach. A toll-free number will be included in the notice.

f. If Healthcare Component determines that the affected individual should be notified urgently of a Breach because of possible imminent misuse of Unsecured PHI, Healthcare Component may, in addition to providing notice as outlined above, contact the affected individual by telephone or other means, as appropriate.

2. **Media Notification**

a. In the case where a single Breach event affects more than 500 residents of a state or jurisdiction, notice shall be provided to prominent media outlets serving that state or jurisdiction. Healthcare Component will make any such media contact pursuant to its media communications policies and procedures.

3. **HHS Notification**

a. Notice will be provided by Healthcare Component without unreasonable delay, and in no case later than 60 days from the Discovery of a Breach, to the Secretary of the Department of Health

and Human Services (HHS) in the manner specified on the HHS website if a single Breach event affects 500 or more individuals.

b. If a Breach affects fewer than 500 individuals, Healthcare Component will maintain a log of the Breach occurrences in any given calendar year and annually will submit the log to HHS in the manner specified on the HHS website no later than 60 days after the end of the calendar year.

4. **Maintenance of Breach Information/Log**. The investigation, report and notice of Breach shall be retained in accordance with this Policy's record retention requirements.

5. **Business Associate Responsibilities**. The Business Associate of the Healthcare Component that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI shall, without unreasonable delay and in no case later than 10 calendar days after discovery of a Breach, notify the Healthcare Component of such Breach. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during such Breach. The Business Associate shall provide the Healthcare Component with any other available information that is required to include in Breach Notification to the individual or, in accordance with HIPAA, thereafter as information becomes available. Upon notification by the Business Associate of discovery of a Breach, the Healthcare Component will be responsible for Breach Notification to affected individuals.

6. **Workforce Training**. The University shall train all members of its Workforce of the Healthcare Component upon hiring and periodically thereafter on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities Workforce members shall also be trained as to how to identify and report Breaches within the University.

a. The University will apply appropriate sanctions against any member of the Workforce who fails to comply with the University's HIPAA Policy.

b. The Department Chairs, Deans, Vice Presidents, Provost and President of the University, with the assistance of the Associate Vice President for Human Resources and Risk Management or its designee, will enforce sanctions against members of the Workforce in accordance with applicable University's policies.

c. The Division of Human Resources will document all sanctions that are applied.

d. **Retaliation**. No employee within the University may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right granted by this Policy. The University may not require individuals to waive their privacy rights as a condition of the provision of Treatment, Payment, enrollment in a health plan, or eligibility for benefits.

XII. ACCOUNTING DISCLOSURES OF PHI

A. Requirements

1. Healthcare Component must provide an individual with an accounting of disclosures in accordance with HIPAA.

2. Healthcare Component must act on an individual's request for an accounting within sixty (60) days of receipt of the request. If a Healthcare Component is unable to provide the accounting within sixty (60) days, it may extend the time period to provide the accounting by no more than thirty (30) days; however, within the original sixty (60) days, the Healthcare Component must provide the individual with a written statement of the reasons for the delay and the date by which Healthcare Component will provide the accounting. Only one extension is permitted per request.

3. The first accounting in a twelve-month period to an individual must be provided without charge. However, Healthcare Component may impose a reasonable cost-based fee for each subsequent request for an accounting made by the same individual within the twelve-month period provided the Healthcare Component informs the individual of the fee prior to complying with the request, thus giving the individual the opportunity to withdraw or modify the request.

4. As part of the accounting of the disclosures, Healthcare Component will coordinate the release of PHI with Business Associates.

5. Healthcare Component must temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides the Healthcare Component with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and it must include the time frame for which such a suspension is required.

6. Healthcare Component must temporarily suspend an individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official, for the time specified by such agency or official, if such agency or official provides the Healthcare Component with an oral statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and it must include the time frame for which such a suspension

is required. However, in as much as the statement was given orally, Healthcare Component must:

a. Document the statement, including the identity of the agency or official making the statement;

b. Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless a written statement is submitted during that time.

7. Requests made for accountings of disclosures of PHI must be made to the individual designated by the Healthcare Component to receive such requests.

B. Responsibilities:

1. An accounting must cover a period of six (6) years, unless a shorter period is requested.

2. The accounting for each disclosure must include:

a. The date of the disclosure;

b. The name and address of the entity or person who received the PHI;

c. A brief description of the PHI disclosed; and

d. A brief statement to reasonably inform the individual of the basis for the disclosure or, in lieu of such statement, a copy of a written request for the disclosure (i.e. subpoena).

3. If a Healthcare Component has made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting with respect to such multiple disclosures should provide:

a. The information required for the first disclosure during the accounting period;

b. The frequency or number of the disclosures made during the accounting period; and

c. The date of the last disclosure during the accounting period.

4. If, during the period covered by the accounting, the Healthcare Component made disclosures of PHI for a particular research purpose in connection with the provision of Treatment in accordance with HIPAA for fifty (50) or more individuals, the accounting may provide:

a. The name of the protocol or other research activity;

b. A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

c. A brief description of the type of PHI that was disclosed;

d. The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

e. The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and

f. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

g. If the Healthcare Component provides an accounting for research disclosures in accordance with this section and it is reasonably likely that the PHI of the individual was disclosed for such research protocol or activity, the Healthcare Component must, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

XIII. DOCUMENT RETENTION, DESTRUCTION AND DISPOSAL

A. The Healthcare Component must document and retain all records in accordance with the University's record retention policy. In addition, the following documents shall be retained pursuant to HIPAA for no less than six (6) years:

1. The designation of Healthcare Components, as set forth in Exhibit A, following any decision to terminate any division or department from the University's Health Care Components. Designations that remain a Health Care Component of the University should be retained permanently.

2. The Notice of Privacy and any subsequent revisions to the Notice from the date of the creation of the Notice, or the date when it last was in effect, whichever is later.

3. The information required to be included in an accounting pursuant to this Policy and HIPAA;

4. The written accounting itself that was given to the requesting individual;

5. The title of positions or offices responsible for receiving and processing requests for an accounting.

6. Records concerning a Breach and notice of Breach, including:

a. A description of what happened, the date of the Breach, date of the discovery of the Breach, and the number of patients affected, if known.

b. A description of the types of unsecured PHI that were involved in the breach (such as full name, Social Security Number, date of birth, home address, account number, etc.).

c. A description of the action taken with regard to notify individuals of the Breach.

d. Resolution of the Breach and steps taken to mitigate the Breach and prevent future occurrences.

7. PHI

B. Records to be maintained under HIPAA will be disposed of properly, in accordance with HIPAA, and the University's record retention requirements.

1. Until such time as destruction or disposal of PHI is permissible, all PHI will be secured against unauthorized or inappropriate access.

2. If utilizing an outside agency for destruction of disposal of PHI, a contract and a Business Associate agreement must be executed between the University and the outside agency. The contract must provide that upon termination, the agency will return or destroy and dispose of all PHI, and provide proof of destruction and disposal and the methodology by which the material was destroyed.

XIV. LIMITED DATA SETS

A. The Privacy Officer may permit the use of PHI to create a Limited Data Set. A Limited Data Set is PHI that excludes certain direct identifiers of the patient, or of the patient's relatives, employers or household members.

1. Limited Data Sets may be used or disclosed only:

a. For the purposes of research, public health, and/or health care operations.

b. To or by a Business Associate for purposes of creating a Limited Data Set for the Healthcare Component or the Business Associate.

2. The Privacy Officer will define methods for creating the Limited Data Set.

B. Processing Requests for Limited Data Sets:

1. Requests for Limited Data Sets must be submitted in writing to the Privacy Officer.

2. A request for a Limited Data Set must include the following:

a. Requestor's name, address, telephone numbers, title, organization or department;

b. Date of request;

c. Purpose of the request (e.g., research, public health or health care operations), including the intended uses, any re-disclosures, and who will use or have access to the Limited Data Set;

d. Names of all recipients of the Limited Data Set;

e. Record parameters or selection criteria – time period included, minimum number of patient records, type of patient records (such as by diagnosis, procedure, drug use, or other criteria); and

f. Date the Limited Data Set is needed.

3. The requestor of a Limited Data Set shall be responsible for submitting payment to the Privacy Officer as reimbursement for the Healthcare Component's resource expenditures related to the request for the Limited Data Set.

4. Request for Limited Data Sets may be denied if:

a. The Healthcare Component cannot create the Limited Data Set;

b. The recipient refuses to compensate the Healthcare Component for generating the Limited Data Set; or

c. Creating the Limited Data Set is an imposition to the operations of the Healthcare Component.

5. The Limited Data Set Request must be reviewed, approved or denied by the Privacy Officer.

6. In the event the request is approved, the requestor will be asked to confirm acceptance of and submit payment for the production costs prior to actual creation of the Limited Data Set. Prior to releasing the Limited Data Set to recipient, Privacy Officer shall require the recipient to execute a written agreement defining the recipient's obligations concerning the Limited Data Set.

XV. BUSINESS ASSOCIATES

A. Business Associates that provide functions, activities, or services for or to Healthcare Component involving use and disclosure of PHI in order to assist Healthcare Component with carrying out Health Care Functions, other than for Treatment, must enter into a Business Associate contract with UCA prior to providing access to such information.

B. Identification of Business Associates:

1. Prior to contracting with any third party, whether an individual or an entity, it is the responsibility of the Healthcare Component to contact the Privacy Officer or his/her designee to determine whether the outside entity or person qualifies as a Business Associate.

2. If a determination is made that the third party is a Business Associate, the Healthcare Component should inquire if the third party will execute a Business Associate Agreement with the University in the form attached as Exhibit F. The Healthcare Component will be responsible for coordinating the execution of Business Associate Agreements. Any changes to the University's form of Business Associate Agreement shall be reviewed and approved by General Counsel.

3. If a Business Associate Agreement is required, the Business Associate Agreement must be signed by both parties before the Business Associate performs any services that involve the use and/or disclosure of PHI.

4. The Privacy Officer should periodically reevaluate the list of Business Associates to determine who has access to PHI in order to assess whether the list is complete and current.

5. The Healthcare Component shall identify systems covered by the Business Associate Agreement.

6. If a third party provides services requiring the use or disclosure of PHI and meets the definition of a Business Associate, and the third party has no known written Business Associate Agreement, Workforce shall notify the Privacy Officer of the need for a Business Associate Agreement. Failure by the using department to assist in obtaining a Business Associate Agreement, where appropriate, may result in disciplinary action.

C. Breach of a Business Associate Agreement:

1. Workforce shall contact the Privacy Officer if a Business Associate has violated a term or obligation of the Business Associate Agreement or any HIPAA requirement(s).

2. If Healthcare Component becomes aware of a violation, Healthcare Component shall notify the Business Associate and the parties will act to mitigate the Breach to the extent practicable. If mitigation is not possible, the Healthcare Component may terminate the Business Associate Agreement and the underlying business arrangements with such vendor that require vendor to use or disclosure PHI, and/or the Privacy Officer will notify the Secretary of HHS.

EXHIBIT A
HEALTH CARE COMPONENT DESIGNATION

The University of Central Arkansas is a public higher education institution created by the laws of Arkansas and is governed by its Board of Trustees. The University is a hybrid entity as defined by HIPAA because a portion of its programs perform covered functions as defined by HIPAA.

In accordance with HIPAA, the following programs are designated as Health Care Components of University of Central Arkansas:

- Student Health Clinic
- Student Counseling Center
- Office of Human Resources
- College of Health and Behavioral Sciences (parts)

Any other University department, division, and program that is not explicitly designated by the University herein as a Health Care Component is not a Healthcare Component under HIPAA.

EXHIBIT B
LIST OF IDENTIFIERS AND DE-IDENTIFICATION PROCESS

A. The University may use PHI where the information that can identify the individual is not present and where there is no reasonable basis to believe that information can be used to identify the individual. The University can create de-identified information by removing or otherwise concealing the following information regarding the individual, relatives, employers, or household members:

1. Names
2. Street address, city, county, precinct, zip code, and equivalent geocodes
3. All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of 90 or older
4. Birth date
5. Telephone numbers
6. Fax numbers
7. Electronic mail addresses
8. Social security number
9. Medical record number
10. Health plan beneficiary number
11. Account numbers
12. Certificate/license number
13. Any vehicle identifiers and serial numbers, including license plate numbers
14. Web Universal Resource Locator
15. Internet Protocol address number
16. Finger or voice prints; biometric identifiers
17. Full face Photographic images; and any comparable images
18. Any other unique identifying number, characteristic, or code that has reason to believe may be identifiable to an anticipated recipient of the information.

EXHIBIT C
DISCLOSURE OF PHI
NO AUTHORIZATION REQUIRED

1. Public Health Activities	Healthcare Components may disclose PHI as follows: 1. To a public health authority that is authorized by law: a. To collect or receive such information for the purpose of preventing or controlling disease, injury or disability; b. To receive reports of child abuse or neglect; 2. To persons subject to the jurisdiction of the Food and Drug Administration with respect to an FDA regulated product or activity for which that person has responsibility for the purpose of activities related to the quality, safety or effectiveness of same. Such purposes include: a. To collect or report adverse events, product defects or problems, or biological product deviations; b. To track FDA regulated products; c. To enable product recalls, repairs, or replacement or lookback; or d. To conduct post-marketing surveillance. 3. To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition if Healthcare Component is authorized by law to notify the person as necessary in the conduct of public health intervention or investigation; or 4. To an employer about an individual who is a member of the Workforce of the employer if: a. Healthcare Component is a covered healthcare provider who provides health care to the individual at the request of the employer to conduct medical surveillance of the workplace or to evaluate individuals for work-related illness or injury; b. The PHI consists of findings concerning work-related illness or injury or workplace related medical surveillance; c. The employer needs the findings to comply with its obligations under federal or state law, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; or d. The healthcare provider gives written notice to the individual that PHI relating to the medical surveillance of the workplace and workplace related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual when the health care is provided or if the healthcare is provided on the worksite of the employer, by posting the notice prominently where the health care is provided. 5. A school, about an individual who is a student or prospective student of the school if: a. The PHI that is disclosed is limited to proof of immunization;

	b. The school is required by State or other law to have such proof of immunization prior to admitting the individual; and c. The Healthcare Component obtains and documents the agreement to the disclosure from either: (i) a parent, guardian or other person acting for a minor; and (ii) the individual if an adult or emancipated minor.
2. Victims of Abuse, Neglect, or Domestic Violence	Except for reports of child abuse or neglect permitted by Section 1 above, Healthcare Component may disclose PHI to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or domestic violence. Such disclosures involving adults are permitted if: a. The disclosure is required by law and the disclosure is limited to the requirements of such law and: (i) Healthcare Component, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victims, or (ii) if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents the PHI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure. b. The individual has been informed about the disclosure unless: (i) the Healthcare Component believes informing the individual would palce the individual at risk of serious harm; or (ii) the Healthcare Component would be informing a personal representative that the Healthcare Component believes is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interest of the individual.
3. Health oversight activities	Healthcare Component may disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or actions; or other activities necessary for the appropriate oversight of: a. the health care system, b. government benefit programs for which health information is relevant to beneficiary eligibility, c. entities subject to government regulatory programs that need health information to determine compliance with program standards, or entities subject to civil rights law that need health information to determine compliance. d. entities subject to civil rights law for which health information is necessary for determining compliance. Healthcare Components may not disclose PHI under this section if an investigation or other activity relates to an individual but does not arise out of and is not directly related to: a. the receipt of health care; b. a claim for public benefits related to health; or c. qualifications for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

4. Judicial and administrative proceedings	All requests for PHI in connection with judicial and administrative proceedings shall be referred to the Office of General Counsel. General Counsel will review the request and respond to the issuer of the request.
5. Law enforcement purposes	Healthcare Components may disclose PHI: 1. As required by law including laws that require the reporting of certain types of wounds or other physical injuries. 2. In compliance with and as limited by the relevant requirements of: a. A court order, warrant, subpoena, or summons issued by a judicial officer; b. A grand jury subpoena; or c. An administrative request, including an administrative subpoena or summons, a civil investigative demand, or similar process authorized under law, provided that: 2. The information sought is relevant and material to a legitimate law enforcement inquiry; 3. The request is as specific and narrowly drawn as is reasonably practicable in light of the purpose for which the information is sought; and 4. De-identified information could not reasonably be used. 5. For the purpose of identifying a suspect, fugitive, material witness, or missing person, Healthcare Component may disclose only the following information: a. Name and Address b. Date and Place of Birth c. Social security number d. ABO blood type and rh factor e. Type of injury f. Date and time of treatment. g. Date and time of death, if applicable, and h. A description of distinguishing physical characteristics like height, weight, gender, race, hair, eye color, facial hair, scars, tattoos. 6. If the disclosure is of the PHI of an individual who is suspected to be a victim of a crime, abuse, or other harm, Healthcare Component may disclose PHI if: a. such information is needed to determine whether a violation of law by a person other than the victim has occurred; and b. immediate law enforcement activity that depends upon obtaining such information would be materially and adversely affected by waiting until the individual is able to agree to the disclosure and c. The disclosure is in the best interest of the individual as determined by the Healthcare Component in the exercise of professional judgment. 7. For purposes of alerting law enforcement of the death of an individual if the covered entity has a suspicion that such death may have resulted from criminal conduct. 8. To alert law enforcement to: a. The commission and nature of a crime

	b. The location of such crime or of the victims of such crime, and c. The identity, description and location of the perpetrator of such crime. 9. If a medical emergency is the result of abuse, neglect or domestic violence of the individual in need of emergency care.
6. Deceased Individuals	The PHI of a deceased individual may be disclosed: a. To a coroner or medical examiner for the purpose of identifying the deceased, determining cause of death, or other duties as authorized by law. b. To funeral directors to carry out their duties; c. To facilitate an organ donation.
7. Research Purposes	1. Healthcare Components may use or disclose PHI for research, regardless of the source of funding of the research, provided that: a. Healthcare Component has obtained a written waiver, in whole or in part, of authorization for use or disclosure of PHI that has been approved by the IRB; and b. The researcher represents that: i. The use or disclosure of PHI is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research; ii. No PHI is to be removed from the Healthcare Component by the researcher in the course of the review; and iii. The PHI for which use or access is sought is necessary for the research. 2. If the research involves a decedent's PHI, the Healthcare Component must obtain from the researcher: a. Representation that the use or disclosure sought is solely for research on the PHI of decedents; b. Documentation of the death of such individual; and c. Representation that the PHI for which the use or disclosure is sought is necessary for research purposes. 3. IRB shall issue a statement identifying the date on which the waiver of authorization was approved. IRB's statement shall include a determination that the waiver of authorization satisfies the following: a. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals based on at least the presence of the following: i. An adequate plan to protect the identifies from improper use and disclosure ii. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and iii. Adequate written assurance that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study or for other research for which the use or disclosure of PHI would be permitted by HIPAA. iv. The research could not practicably be conducted with the waiver or alteration; and v. The research could not practicably be conducted without access to and use of the PHI. b. A brief description of the PHI for which use or access has been determined to be necessary for the IRB.

	c. The alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures as required by law. d. Approval is indicated by signature of the chair or other member as designated by the chair of the IRB.
8. Emergency Circumstances to Avert Threats to Safety	1. Healthcare Components may, consistent with applicable law and standards of ethical conduct and based on a reasonable belief that the use or disclosure is: a. necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual and is to a person reasonably able to prevent or less the threat, including target of the threat; or b. necessary for law enforcement to identify or apprehend an individual based upon a statement by an individual admitting participation in a violent crime that the Healthcare Component reasonably believes may have caused serious physical harm to the victim or where it appears from the circumstances that the individual has escaped from a correctional institution or from lawful custody. 2. Disclosure of PHI may not be made if learned by Healthcare Component: a. In the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure; or b. Through a request by the individual to initiate or to be referred for treatment, counseling or therapy. 3. Specific information that may be disclosed is limited by HIPAA.
9. Specialized Government Functions	Disclosure of PHI may be made in connection with military and veteran activities, national security and intelligence activities, protective services for the President and others, medical suitability for the U.S. Department of State, to obtain security clearance, and correctional institutions and other law enforcement custodial situations, and to government programs providing benefits. In the event PHI is needed for such a purpose, the Privacy Officer must be consulted prior to making such a disclosure, and any disclosure of PHI shall comply with HIPAA.

EXHIBIT D

AUTHORIZATION FORM

[Insert PDF form]

Student Health Clinic

THE UNIVERSITY OF CENTRAL ARKANSAS
201 Donaghey Avenue
Student Health Building – 1st Floor
Conway, AR 72035-0001
Phone: (501) 450-3136
Fax: (501) 450-3370

PERMISSION FOR RELEASE OF INFORMATION

In compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Student Health Clinic of the University of Central Arkansas requires your written consent before disclosing any personal information. Your consent to share this information may be withdrawn in writing at any time, so long as such documents are specific as to information covered, dated, and signed.

I, _____, ID# _____, request
(Print Name) (DOB, Student ID#, or SSN)

Please choose one:

☐ University of Central Arkansas Student Health Clinic, or

☐ _____, Fax# _____
Name of Institution/Business

Release the following information from my health record: (Check all that apply)

☐ Immunization Record ☐ Lab Results ☐ Women's Health Record ☐ Entire Medical Record

☐ Care delivered on specific date ___ / ___ / ___ ☐ Care delivered for _____ only.
(Specific illness/injury)

Please release requested information to:

☐ **Student Health Clinic**
University of Central Arkansas
Student Health Building – 1st Floor
201 Donaghey Avenue
Conway, Arkansas 72035-0001
Ph#: (501) 450-3136
Fax#: (501) 450-3370
E-mail: shc@uca.edu

OR:

_____
Name

_____
Address

_____
City/State/Zip

_____
Telephone Number

Please check return delivery method:

☐ Mail to above address

☐ Fax to _____

☐ E-mail to _____
(Note: Emails may not be protected by the HIPAA privacy rule)

_____
Patient's Signature Date

_____
Contact Info (used only for questions regarding above request)

_____
Witness By (SHC Staff)

EXHIBIT E

NOTICE OF PRIVACY PRACTICES & ACKNOWLEDGMENT OF RECEIPT

NOTICE OF PRIVACY PRACTICES

[Insert PDF Form]

UCA Student Health Clinic Privacy Statement

Your Information, Your Rights, Our Responsibilities

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully.

You have the right to:

- Get a copy of your paper or electronic medical record
- Request confidential communication
- Ask us to limit the information we share
- Get a copy of this privacy notice
- Choose someone to act for you
- File a complaint if you believe your privacy rights have been violated

You have some choices in the way that we use and share information as we:

- Tell family and friends about your condition

Our Uses and Disclosures

We may use and share your information as we:

- Treat you
- Help with public health and safety issues
- Comply with the law
- Respond to organ and tissue donation requests
- Work with a medical examiner
- Address workers' compensation, law enforcement, and other
- government requests
- Respond to lawsuits and legal actions

Your Rights—

When it comes to your health information, you have certain rights.
This section explains your rights and some of our responsibilities to help you.

Get an electronic or paper copy of your medical record

- You can ask to see or get an electronic or paper copy of your medical record and other health information we have about you.
- We will provide a copy or a summary of your health information, usually within 30 days of your request.

Request confidential communications

- You can ask us to contact you in a specific way (for example, home or office phone) or to send mail to a different address.

Ask us to limit what we use or share

- You can ask us not to use or share certain health information for treatment, payment, or our operations. We are not required to agree to your request, and we may say "no" if it would affect your care.

Get a copy of this privacy notice

You can ask for a paper copy of this notice at any time, even if you have agreed to receive the notice electronically. We will provide you with a paper copy promptly.

Choose someone to act for you

- If you have given someone medical power of attorney or if someone is your legal guardian, that person can exercise your rights and make choices about your health information.
- We will make sure the person has this authority and can act for you before we take any action.

File a complaint if you feel your rights are violated

- You can complain if you feel we have violated your rights by contacting us directly.
- You can file a complaint with the U.S. Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting ***www.hhs.gov/ocr/privacy/hipaa/complaints***.
- We will not retaliate against you for filing a complaint.

Your Choices—

For certain health information, you can tell us your choices about what we share. If you have a clear preference for how we share your information in the situations described below, talk to us. Tell us what you want us to do, and we will follow your instructions. In these cases, you have both the right and choice to tell us to:

- Share information with your family, close friends, or others involved in your care
- Share information in a disaster relief situation

If you are not able to tell us your preference, for example if you are unconscious or incoherent, we may share your information if we believe it is in your best interest. We may also share your information when needed to lessen a serious and imminent threat to health or safety.

Our Uses and Disclosures

How do we typically use or share your health information?

We typically use or share your health information in the following ways.

Treat you

- We can use your health information and share it with other professionals who are treating you. *Example: A doctor treating you for an injury asks another doctor about your overall health condition.*

Run our organization

- We can use and share your health information to run our practice, improve your care, and contact you when necessary. *Example: We use health information about you to manage your treatment and services.*

How else can we use or share your health information?

We are allowed or required to share your information in other ways – usually in ways that contribute to the public good, such as public health. We have to meet many conditions in the law before we can share your information for these purposes.
For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

Help with public health and safety issues

- We can share health information about you for certain situations such as:
- Preventing disease such as infectious outbreaks on campus
- Reporting adverse reactions to medications
- Reporting suspected abuse, neglect, or domestic violence
- Preventing or reducing a serious threat to anyone's health or safety

Comply with the law

We will share information about you if state or federal laws require it, including with the Department of Health and Human Services if it wants to see that we are complying with federal privacy law.

Respond to organ and tissue donation requests

We can share health information about you with organ procurement organizations if you agreed to be an organ donor.

Work with a medical examiner or funeral director

We can share health information with a coroner, medical examiner, or funeral director when an individual dies.

Address workers' compensation, law enforcement, and other government requests

We can use or share health information about you:

- For workers' compensation claims
- For law enforcement purposes or with a law enforcement official
- With health oversight agencies for activities authorized by law
- For special government functions such as military, national security, and presidential protective services

Respond to lawsuits and legal actions

We can share health information about you in response to a court or administrative order, or in response to a subpoena.

Our Responsibilities—

- We are required by law to maintain the privacy and security of your protected health information.
- We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information.
- We must follow the duties and privacy practices described in this notice and give you a copy of it.
- We will not use or share your information other than as described here unless you tell us we can in writing. If you tell us we can, you may change your mind at any time. Let us know in writing if you change your mind.

For more information see: www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/noticepp.html.

Changes to the Terms of this Notice

We can change the terms of this notice, and the changes will apply to all information we have about you. The new notice will be available upon request, in our office, and on our web site.

Other:

- We never market or sell personal information.
- This policy was approved by Dr. Randy Pastor on 10/1/2017

EXHIBIT F

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement is made effective on the _____ of _____, 20__ by and between _____ located at _____, herein after referred to as "Business Associate" and the ***Board of Trustees of the University of Central Arkansas*** located at ***201 Donaghey Avenue, Conway, Arkansas 72035,*** hereinafter referred to as "Covered Entity" (collectively referred to as "Parties").

WHEREAS, Sections 261 through 264 of the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, known as "the Administrative Simplification provisions," direct the Department of Health and Human Services to develop standards to protect the security, confidentiality and integrity of health information; and pursuant to the Administrative Simplification provisions, the Secretary of Health and Human Services issued regulations modifying 45 CFR Parts 160 and 164 (the "HIPAA Security and Privacy Rule"); and

WHEREAS, the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), pursuant to Title XIII of Division A and Title IV of Division B, called the "Health Information Technology for Economic and Clinical Health" ("HITECH") Act, provides modifications to the HIPAA Security and Privacy Rule (hereinafter, all references to the "HIPAA Security and Privacy Rule" are deemed to include all amendments to such rule contained in the HITECH Act and any accompanying regulations, and any other subsequently adopted amendments or regulations); and

WHEREAS, the Parties wish to enter into or have entered into a service agreement or contractual arrangement whereby Business Associate will provide certain services to the Covered Entity and whereby Covered Entity may provide Business Associate with Protected Health Information ("PHI") or Business Associate may create or receive PHI on behalf of Covered Entity (the agreement evidencing such arrangement is entitled _____ dated _____ and is hereinafter referred to as "Agreement"); and

THEREFORE, in consideration of the Parties' continuing obligations under the Agreement, compliance with the HIPAA Security and Privacy Rule, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, and intending to be legally bound, the Parties agree to the provisions of this Agreement in order to address the requirements of the HIPAA Security and Privacy Rule and to protect the interests of both Parties.

1. Definitions

Except as otherwise defined herein, any and all capitalized terms in this Section shall have the definitions set forth in the HIPAA Security and Privacy Rule. In the event of an inconsistency between the provisions of this Agreement and mandatory provisions of the HIPAA Security and Privacy Rule, as amended, the HIPAA Security and Privacy Rule shall control. Where provisions of this Agreement are different than those mandated in the HIPAA Security and Privacy Rule, but are nonetheless permitted by the HIPAA Security and Privacy Rule, the provisions of this Agreement shall control.

The term "Protected Health Information" means individually identifiable health information including, without limitation, all information, data, documentation, and materials, including without limitation, demographic, medical and financial information, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. "Protected Health Information" includes without limitation "Electronic Protected Health Information" as defined below.

The term "Electronic Protected Health Information" means Protected Health Information which is transmitted by Electronic Media (as defined in the HIPAA Security and Privacy Rule) or maintained in Electronic Media.

The term "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR 164.103.

2. Permitted Uses and Disclosures by Business Associate

Except to the extent that a use or disclosure would violate the HIPAA Security and Privacy Rule if such use or disclosure were done by the Covered Entity, Business Associate may use or disclose PHI to the extent reasonably necessary and in compliance with 45 CFR § 164.502(b) regarding the minimum necessary requirements:

(a) to perform functions, activities, or services for, or on behalf of, Covered Entity as set forth in the Agreement;

(b) for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached;

(c) to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1); and

(d) to provide Data Aggregation services to Covered Entity, if requested by Covered Entity, and as permitted by 42 CFR 164.504(e)(2)(i)(B).

3. Obligations of Business Associate

(a) Business Associate agrees to not use or further disclose PHI other than as permitted by this Agreement or as Required By Law.

(b) Associate agrees to implement administrative, physical, and technical safeguards that (i) prevent use or disclosure of the PHI other than as provided for by this Agreement and (ii) reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of Covered Entity; and ensure that any agent, including a subcontractor, to whom Business Associate provides such information agrees to implement reasonable and appropriate safeguards to protect it. Business Associate agrees at the request of Covered Entity to employ technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals that are consistent with National Institute of Standards and Technologies (NIST) Special Publications.

(c) Business Associate agrees to, following the discovery of a Breach of Unsecured PHI, as defined in the HIPAA Security and Privacy Rule, notify the Covered Entity of such Breach pursuant to the terms of 45 CFR § 164.410 and cooperate in the covered entity's breach analysis procedures, including risk assessment, if requested. A Breach shall be treated as discovered by Business Associate as of the first day on which such Breach is known to Business Associate or, by exercising reasonable diligence, would have been known to Business Associate. Business Associate will provide such notification to Covered Entity without unreasonable delay and in no event later than sixty (60) calendar days after discovery of the breach. Such notification will contain all of the elements required in 45 CFR § 164.410. The Parties agree that Business Associate is not an Agent of Covered Entity.

(d) Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Breach of Unsecured PHI or other use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

(e) Business Associate agrees to ensure that any agent of Business Associate, including a subcontractor, to whom it provides PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply to this Agreement to Business Associate with respect to such information.

(f) To the extent Business Associate maintains any PHI in a Designated Record Set, and such information is not also in the possession of Covered Entity, Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner required under the HIPAA Regulations, such PHI to Covered Entity or as directed by Covered Entity, to an individual authorized by state or federal law to receive the information, in order to meet the requirements under 45 C.F.R. § 164.524.

(g) To the extent Business Associate maintains any PHI in a Designated Record Set, Business Associate agrees to make any amendments to the PHI that Covered Entity has agreed to pursuant to 45 C.F.R. § 164.526, upon notification by Covered Entity to Business Associate that such information requires amendment.

(h) Business Associate agrees to make internal practices, books, and records, including policies and procedures and PHI, relating to the use and disclosure of Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary of the United States Department of Health and Human Services or his/her designee solely for the purposes of determining Covered Entity's compliance with the HIPAA Regulations.

(i) Business Associate agrees to make available to Covered Entity Protected Health Information in response to a request for an accounting of disclosures required by 45 C.F.R § 164.528. Business Associate also agrees to document its disclosures of the PHI, if any, and information related to such disclosures, as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of Protected Health Information pursuant to 45 C.F.R § 164.528. In the event of such a request, Business Associate agrees to provide to Covered Entity or to the requesting party, in the time and manner required by 45 C.F.R. § 164.528, an accounting of any such disclosures.

(j) Business Associate agrees to not directly or indirectly receive remuneration in exchange for any PHI that it receives from or on behalf of Covered Entity.

(k) Business Associate agrees not to make or cause to be made any written fundraising communication that is prohibited by the HIPAA Privacy and Security Rule.

(l) Any healthcare providers employed by Business Associate who will be providing treatment to UCA patients through the Agreement or this Business Associate Agreement will follow all UCA HIPAA Privacy and Security Policies. Failure to follow these policies will constitute a material breach of this Business Associate Agreement.

4. Obligations of Covered Entity

(a) Covered Entity agrees to notify Business Associate of any limitations in its Notice of Privacy Practices to the extent that Covered Entity determines that such limitation may affect Business Associate's use or disclosure of PHI.

(b) Covered Entity agrees to notify Business Associate of any changes in, or revocation of, permission by the patient to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c) Covered Entity agrees to notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

(d) Covered Entity agrees to notify Business Associate of any amendments made or required to be made to PHI in the possession of Business Associate, pursuant to 45 C.F.R. § 164.526.

5. Term and Termination.

(a) Except for termination for cause as set forth below, the Term of this Business Associate Agreement shall be effective as of the effective date stated herein and shall continue for each year thereafter until the Parties agree otherwise in writing, signed by persons authorized to execute such agreements, and as long as the Business Associate ceases to receive, use, create, disclose or maintain any PHI on behalf of Covered Entity. For such termination to be effective, such PHI must have been destroyed by Business Associate or returned to Covered Entity in accordance with the terms of Paragraph 5(c).

(b) Upon Covered Entity's knowledge of a material breach by Business Associate of the terms of this Business Associate Agreement, Covered Entity shall have the right to (i) terminate immediately the Agreement and this Business Associate Agreement; or (ii) provide an opportunity for Business Associate to cure the breach or end the violation within the time specified by Covered Entity, and if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, then Covered Entity may terminate the Agreement and this Business Associate Agreement.

(c) Covered Entity may terminate this Business Associate Agreement for any reason with 90 days notice. Except as provided in this Business Associate Agreement, upon termination of this Business Associate Agreement for any reason,

Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, including any copies of such PHI. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate.

In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as BUSINESS ASSOCIATE maintains such Protected Health Information.

6. Miscellaneous.

(a) **Incorporation into Agreement.** The Parties agree that this Business Associate Agreement is incorporated into and made part of the Agreement.

(b) **Construction of Terms.** To the extent they are not clear, the terms of this Business Associate Agreement shall be construed to allow for compliance by both Parties with the HIPAA Security and Privacy Rule.

(c) **Amendment.** The Parties agree to take such action as is necessary to amend this Business Associate Agreement from time to time for the parties to comply with the requirements of the HIPAA Regulations. All other amendments to this Business Associate Agreement agreed upon by the parties must be in writing and signed by both parties.

(d) **Waiver.** The failure of either Party to enforce at any time any provision of this Agreement shall not be construed to be a waiver of such provision, nor in any way to affect the validity of this Business Associate Agreement or the right of either Party thereafter to enforce each and every such provision

(e) **No Third Party Beneficiaries.** Nothing in this Business Associate Agreement shall confer upon any person other than the Parties and their respective successors or assigns any rights, remedies, obligations or liabilities.

(f) **Jurisdiction/Governing Law.** Any disputes concerning or arising out of this Business Associate Agreement shall be adjudicated or heard in Arkansas in a court, tribunal, or other administrative or judicial proceeding with competent jurisdiction. To the extent state law applies to this Business Associate Agreement, or the application and interpretation of this Business Associate Agreement, the law of Arkansas shall govern without regard to its choice of law principles.

(g) **Notices.** Notices permitted or required to be given hereunder shall be provided to:

Dr. Graham Gillis
UCA Privacy Officer
201 Donaghey Avenue; Wingo Hall Rm. 103
Conway, AR 72035
Fax: (501) 450-5088
Telephone: (501) 450-5051

(h) **University of Central Arkansas Contract Rider**

Notwithstanding any other provision of this agreement or contract, the University of Central Arkansas shall not be responsible or liable for any type of special or consequential damage to the other party, specifically including, but not limited to, lost profits or commissions, loss of goodwill, or any other damages of such nature.

Notwithstanding any other provision of this agreement or contract, the University of Central Arkansas shall never indemnify or hold another party harmless from any damages, liability, claims, demands, causes of action or expenses. However, with respect to any loss, expense, damage, liability, claim or cause of action, either at law or in equity, for actual or alleged injuries to persons or property, arising out of any negligent act or omission by UCA, or its employees or agents, in the performance of this agreement, UCA agrees that:

(a) It will cooperate with the other party to this agreement in the defense of any action or claim brought against the other party seeking damages or relief;

(b) It will, in good faith, cooperate with the other party to this agreement should such other party present any claims or causes of action of the foregoing nature against UCA to the Arkansas State Claims Commission;

(c) It will not take any action to frustrate or delay the prompt hearing on claims of the foregoing nature by the Arkansas State Claims Commission, and will make reasonable efforts to expedite any hearing thereon.

UCA reserves the right, however, to assert in good faith any and all defenses available to it in any proceedings before the Arkansas State Claims Commission or any other forum. Nothing herein shall be interpreted or construed to waive the sovereign immunity of UCA."

The University of Central Arkansas does not have any form of general liability insurance. It does have liability insurance coverage on vehicles, as well as certain professional liability coverage for clinical programs (and students assigned through those programs). Please contact the university department with responsibility for the program involved or the Office of General Counsel, if you have questions concerning insurance coverage.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement to be effective as of the Effective Date.

[Insert Business Associate]	***Board of Trustees of the University of Central Arkansas***
Telephone Number: _____	
Federal ID Number or SSN: _____	
By: _____	By: _____
Print Name: _____	Print Name:
Print Title: _____	Print Title: _____
Date: _____	Date: _____