June 13, 2011
The University of Arizona

HIPAA Privacy and Security Policy

1. INTRODUCTION

The University of Arizona (UA) is committed to protecting the privacy, confidentiality, and security of Protected Health Information (PHI) as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act (2010). These are federal laws that, in part, protect the privacy of individually identifiable patient information and provide for the electronic and physical security of health and patient medical information. Privacy and security are addressed separately in HIPAA under two distinct rules, the Privacy Rule and the Security Rule.

The Privacy Rule sets the standards for how PHI should be controlled. Privacy standards define what information must be protected, who is authorized to access, use, or disclose this information, what processes must be in place to control the access, use, and disclosure of information, and to ensure patient privacy rights.

The Security Rule sets the standards that require covered entities and business associates to implement basic security safeguards to protect electronic PHI. Security standards specify who has access to electronic health information and how to protect it from accidental or intentional disclosure to unauthorized persons. The standards include administrative, technical, and physical safeguards.

The University of Arizona identifies itself as a “hybrid entity” as defined in the HIPAA Privacy Rule.

A HIPAA hybrid entity is a single legal entity that is not fully a healthcare provider, clearinghouse or insurer, but has one or more units that perform one or more of these HIPAA-covered functions. Only the HIPAA-covered functions of the hybrid entity are subject to the HIPAA Privacy and Security Rules.

Under the hybrid entity designation, the UA must define and designate its covered healthcare component(s). The UA covered healthcare component(s) must comply with the HIPAA Privacy and Security Rules. Currently the UA has designated the following covered healthcare component(s) under its HIPAA hybrid entity status:

- Recovery Through Integration, Support and Empowerment (RISE) center in the UA College of Medicine Family & Community Medicine Department

The Privacy Officer will periodically review the status of UA units to determine whether this list of covered healthcare components of the UA hybrid entity should be revised.
Additionally, certain University units are considered Business Associates of a HIPAA-covered entity such as UA Healthcare; thus, these UA units as Business Associates are responsible for compliance with HIPAA, as required by the HITECH Act.

This policy will be reviewed periodically to ensure compliance with HIPAA, HITECH and other applicable laws and appropriately update its content to address relevant changes in operations or UA’s covered entity status. Additionally, all University centers, clinics, departments or programs that provide health-related services or conduct health-related activities shall notify the Privacy Officer before engaging in any HIPAA standard transactions or other electronic transactions in order for the Privacy Officer to conduct an analysis to determine whether the proposed electronic transactions would trigger identification as a covered entity under HIPAA.

2. DEFINITIONS

Authorization: An authorization is a written permission for a defined use and/or disclosure of an individual’s PHI for purposes other than treatment, payment or other healthcare transactions. An authorization must contain specific elements required by HIPAA and be approved by the Institutional Review Board (for any disclosures related to research) or the Privacy Officer, as appropriate.

Business Associate: A Business Associate is an external person or entity that performs certain functions, activities, or services on behalf of a HIPAA-covered unit when that function, activity or service involves the use and/or disclosure of PHI.

De-identified PHI: De-identified PHI is information that has been stripped of its identifiable information and meets the HIPAA criteria for de-identification. In order for PHI to be considered “De-Identified,” it must NOT include any of the following elements:

a. Names
b. All geographic subdivisions smaller than a state including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
c. All element of dates (except year) for dates directly related to an individual, including birth date, admission/discharge dates, date of death, and, for persons over 89 years of age, all dates including year indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
d. Telephone numbers
e. Fax numbers
f. Electronic mail addresses
g. Social Security numbers
h. Medical record numbers  
i. Health plan beneficiary numbers  
j. Account numbers  
k. Certificate/license numbers  
l. Vehicle identifiers and serial numbers and license plates  
m. Device identifiers and serial numbers  
n. URLs  
o. IP addresses  
p. Biometrical identifiers, including voice and fingerprints  
q. Full face photographic images and any other comparable images  
r. Any other unique identifying number, characteristic, or code except for secure reidentification or data matching codes that are not derived from information about the individual.

**Minimum Necessary:** The “minimum necessary” standard applied when using or disclosing PHI or when requesting PHI from another covered unit or external entity. A covered University unit or one serving as a business associate of a covered entity must make reasonable efforts to limit access (both internally and externally) to PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure.

**Protected Health Information (PHI):** PHI, as defined by HIPAA, means individually identifiable health information that, except as provided in part (g) of this definition, is transmitted by electronic media, maintained in electronic media or transmitted or maintained in any other form or medium and includes the following:

a. A subset of health information, including demographic information collected from an individual; and  
b. Is oral or recorded in any form or medium; and  
c. Is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and  
d. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and  
e. That identifies the individual; or  
f. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.  
g. PHI does NOT include the following:  
   (1) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;  
   (2) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and  
   (3) Employment records held by a covered entity in its role as employer.

**Research:** Research is a systematic investigation designed to develop or contribute to generalizable knowledge. The use of PHI in a research study requires a signed authorization from the patient or waiver issued by the Institutional Review Board.
Privacy Officer: The UA has a designated Privacy Officer. As required by HIPAA, the Privacy Officer is responsible for the development and implementation of policies and procedures necessary for UA’s covered components (if any) and departments or units serving as a Business Associate to comply in full with the HIPAA Privacy Rule. The Privacy Officer shall survey and monitor UA’s compliance with the HIPAA Privacy Rule on an ongoing basis. Changes to the HIPAA status of the UA shall be made by the Privacy Officer, in consultation with the Office of the General Counsel.

The Privacy Officer is authorized to receive, investigate, and recommend resolution of complaints concerning UA’s compliance with the HIPAA Privacy rule and to provide information about Notice(s) of Privacy Practices. When investigating a possible privacy breach, the Privacy Officer may convene a team of appropriate representatives from other units to assist in the investigation and analysis of evidence.

Security Officer: The UA Information Security Officer will serve as the UA HIPAA Security Official for this policy. As required by HIPAA and the HITECH Act, the Security Officer and Privacy Officer will work together to develop, implement, and maintain policies and procedures necessary for UA’s covered components (if any) and business associate units to comply with the Security Rule, including those necessary to establish and maintain administrative, physical and technical security safeguards and to prevent, detect, contain, and correct security violations. The Security Officer and Privacy Officer shall monitor UA’s covered components for compliance with the Security Rule. The Security Officer is designated to receive, investigate, recommend resolution, and respond to possible breaches of the Security Rule.

3. SCOPE

This policy applies to all members of UA faculty, staff, students, and volunteers who work or train in units that serve as Business Associates for a covered entity or are identified as engaging in HIPAA standard transactions. Additionally, the Privacy Officer is responsible for establishing and enforcing this policy and the HIPAA Compliance Program as described in “Additional Policy Components” of this Policy. All Vice Presidents, Deans, Directors, and Department Heads have the management authority and are expected to take appropriate actions to comply with this policy and supporting procedures and standards where applicable.

4. PHYSICAL AND ELECTRONIC SECURITY

HIPAA requires physical and electronic security measures to maintain the privacy of PHI. This requirement includes limiting physical and electronic access to PHI in all forms, including written, spoken, pictorial, electronic recording, or printed. See security
requirements contained in the UA Information Security Policy at http://security.arizona.edu/policy.

5. PRIVACY AND SECURITY BREACHES

If any UA employee or contractor becomes aware of an actual or alleged breach of this policy, the employee or contractor is required to report the actual or alleged breach to the UA Privacy Officer or UA Information Security Officer. Additionally, the Privacy Officer may receive reports from anyone else regarding an actual or alleged breach.

UA will mitigate, to the extent practicable, any violation of this policy or any other applicable requirements of HIPAA.

Faculty and staff members found to have violated this policy will be subject to disciplinary action, up to and including dismissal, under the applicable UA disciplinary policies. Students in violation of this policy will be subject to disciplinary action under the applicable student policies and procedures. In addition, individuals who are in violation of HIPAA may be subject to civil and criminal penalties as provided by law.

Additional Policy Components

HIPAA Compliance Program

The HIPAA Compliance Program (HCP) will be documented on the UA HIPAA website. The Privacy Officer is responsible for maintenance and updates to this website. The HCP will encompass HIPAA training requirements, compliance reviews, and privacy complaint and breach investigation processes, as well as other components the Privacy Officer deems necessary.

Investigation of Possible Breaches

When notified of a potential privacy or security breach, the Privacy Officer and/or the Security Officer, will conduct an investigation. Additionally, the Privacy Officer may coordinate such investigation with representatives from other units, as appropriate, including but not limited to the Information Security Advisory Committee (UA-ISAC) (see, http://security.arizona.edu/isac).

All UA faculty, staff, students and volunteers are required under the conditions of their employment or status to cooperate in all investigations and to respond to inquiries from the Privacy Officer and Security Officer in a prompt manner. Failure to cooperate with a privacy or security breach investigation may result in disciplinary action by the University, in accordance with applicable policies. See the HCP for more information regarding breach investigations.
Coordination with UA Healthcare

UA Healthcare and the UA may coordinate activities to assist both organizations with training, PHI access and use and disclosure, electronic security, and other HIPAA-related processes.

Administrative, Physical and Technical Safeguards

Each department or unit that accesses or maintains PHI is required to develop procedures to safeguard the security of the PHI. Examples may include locked files with access limited to those who require the information to perform their jobs, fax machines that receive PHI must be placed in a non-public location, and protection of computer screens on which PHI is displayed from being viewed by passers-by.

The electronic transmission of PHI should employ the encryption techniques described under the UA Information Security Policy: http://security.arizona.edu/policy.

Disposal of PHI in paper format or computer diskettes must be discarded in designated shred bins. For PHI in other formats, follow the University of Arizona procedures for destruction.

Student Health Information

Student health information obtained or created as part of the student’s academic career is normally covered under the privacy provisions of the “Family Educational Rights and Privacy Act” (FERPA). This policy in no way affects the applicability of FERPA regulations to student records, including student health records created as a result of healthcare services provided by UA Campus Health Service or other campus clinics, programs, or centers. For more information on student privacy, see www.registrar.arizona.edu/privacyguidelines.htm.

Training

The Privacy Officer, in conjunction with the Security Officer and other training staff, will identify and develop content and educational programs as appropriate. Specific training requirements and opportunities will be set forth in the Privacy Officer’s HCP.

Training for UA employees who have access to electronic health records or other electronic systems may be coordinated with UA Healthcare or other organizations that are responsible for granting access to and monitoring the security of their data.