Policy Contents

Policy Information

Effective Date:
October 12, 2013
Last Revised Date:
March, 2016
Policy Number:
Res-200
Responsible Unit:
HIPAA Privacy Program
Phone:
(520) 621-1465
Email:
privacyoffice@email.arizona.edu [1]

Purpose and Summary

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 and associated regulations (see Code of Federal Regulations (CFR) 45 Parts 160, 162 and 164) were enacted in part to establish rights for patients and responsibilities for Covered Entities and Business Associates of Covered Entities with regard to the confidentiality, availability, and integrity of Protected Health Information (PHI).

Pursuant to the statute and regulations, organizations that are Hybrid Entities must designate certain segments of their organizations as Health Care Components and take all reasonable steps to assure compliance within the Health Care Component with all applicable HIPAA Privacy, Security, and Breach Notification Rules and regulations promulgated in the Health Insurance Portability and Accountability Act (HIPAA) and Title XIII, Subtitle D of the Health Information Technology for Economic and Clinical Health (HITECH) Act (HIPAA and HITECH may be collectively referred to as "HIPAA").

The University is a Hybrid Entity, as defined by HIPAA (see 45 CFR § 164.103). For the purpose of this Policy, University Health Care Components consist of those programs that meet the definitions of "Covered Entity" or "Business Associate," as defined by 45 CFR § 160.103, and as determined by the University HIPAA Privacy Officer and the Senior Director for Human & Clinical Research Services.

Additionally, organizations performing work for or on behalf of Covered Entities, and which meet the definition of a Business Associate, must establish Business Associate Agreements and comply with the applicable HIPAA Rules.

The purpose of this policy is to:

1. Designate the University of Arizona (UA or the University) as a Hybrid Entity;
2. Acknowledge that the University performs certain activities that meet the definitions of a "Covered Entity" and "Business Associate";
3. Establish a broad operational framework for the Privacy, Security, and Breach Notification Rules found in HIPAA; and
4. Ensure all members of the University community understand their rights and obligations with regard to the privacy, security, and integrity of PHI.

Scope

This policy applies to the entire University.

Definitions

All capitalized terms in this Policy have the same definitions found in HIPAA (45 CFR Parts 160 and 164).

Policy

A. UA Community Obligations

1. **General Statement**: This Policy, including provisions related to breach reporting, investigation, and remediation, applies to all University Health Care Component Workforce members, which include employees, students, affiliates, associates, volunteers, trainees, and visiting scholars and researchers; and to all other persons whose conduct, in the performance of work for a Health Care Component, is under the direct control of such Health Care Component, whether or not they are paid by the Health Care Component. All Vice Presidents, Deans, Directors, Department Heads, and others in leadership or management roles are expected to take appropriate actions, when applicable, to comply with this Policy and supporting procedures and standards.
2. **Reporting Breaches:** If ***any*** University Workforce member becomes aware of an actual or alleged breach of HIPAA requirements or this Policy, including but not limited to a privacy breach or breach of electronic PHI, the individual is ***required*** to report the actual or alleged breach to the University HIPAA Privacy Officer. Additionally, any member of the public may provide notification to the University HIPAA Privacy Officer regarding an actual or alleged breach of HIPAA requirements or of this Policy. The University HIPAA Privacy Officer will provide information on its website to enable the reporting of actual or alleged breaches and will develop procedures to ensure the prompt and timely response to reports received by the

University HIPAA Privacy Officer.

The University will mitigate, as required by applicable law, any violation of this policy or applicable HIPAA requirements.

University Workforce members found to have violated this Policy may be subject to disciplinary action, up to and including dismissal, under the applicable University disciplinary policies. Students in violation of this policy may be subject to disciplinary action under the applicable student policies and procedures. Individuals who are in violation of HIPAA regulations may be subject to civil and criminal penalties as provided by law.

3. **Potential Breach or Noncompliance Investigations**: When the University HIPAA Privacy Officer is notified of a potential privacy or security breach, or a potential breach of this Policy, the University HIPAA Privacy Officer will promptly investigate and will recommend appropriate corrective actions in the event that a breach has occurred. The University HIPAA Privacy Officer may involve the University Information Security Officer, as appropriate, and in such case, the University HIPAA Privacy Officer and the University Information Security Officer will conduct an investigation. In the event the University Information Security Officer receives notification of a potential HIPAA breach or breach of this policy, the University Information Security Officer will promptly notify the University HIPAA Privacy Officer.

   Nothing in this policy precludes the applicability of UA and/or ABOR policies that relate to the investigation of cyber-security incidents.

   All University Workforce members will cooperate in such investigations and promptly respond to inquiries from the University HIPAA Privacy Officer and/or University Information Security Officer. Failure to cooperate with an investigation concerning a privacy or security breach, or a breach of this policy, may result in disciplinary action by the University, in accordance with applicable policies.
4. **Prior Notification of Intent to Conduct HIPAA Standard Transactions**: All University colleges, centers, departments, programs or individuals must notify the University HIPAA Privacy Officer of their intent to engage in HIPAA standard transactions or to send, receive, and/or maintain PHI in connection with the provision of health care services (see 45 CFR § 160.103). Notification must be as soon as possible **prior** to proposed initiation of such transmissions, but no later than ninety (90) days prior to the planned date of implementation in order to enable the University HIPAA Privacy Officer and/or University Information Security Officer to conduct an analysis and recommend appropriate HIPAA compliance measures.

B. Organizational Guidelines

The University **HIPAA Privacy Officer,** who leads the **HIPAA Privacy Program** (HPP) as part of the Office for Research and Discovery (ORD), is charged with implementing this Policy and overseeing the University's HIPAA compliance program, which includes developing standard procedures, preparing and disseminating information and training materials, monitoring and auditing, and responding to reports of suspected noncompliance with this Policy or with HIPAA requirements to prevent further similar offenses upon detection of a violation. The HPP will work with University Information Security (UAIS) to ensure compliance with rules regarding the security, availability, and integrity of electronic PHI in the possession of Health Care Components.

1. **University HIPAA Privacy Officer & University Information Security Officer:**
   a. University HIPAA Privacy Officer: The University HIPAA Privacy Officer oversees all

ongoing activities related to the University's implementation of this Policy and is designated as the individual primarily responsible for ensuring the University's HIPAA compliance. The University HIPAA Privacy Officer is responsible for maintaining relevant procedures, guidelines, and forms; maintaining the University HIPAA Privacy Program website; and developing HIPAA training and educational materials.

The University HIPAA Privacy Officer reports to the Senior Director of Human & Clinical Research Services.

The University HIPAA Privacy Officer will coordinate with the University Information Security Officer to ensure and otherwise achieve compliance with all applicable HIPAA Security and Breach Notification Rules.

The HIPAA Privacy Officer serves as the University's chief point of contact with the U.S. Department of Health and Human Services Office for Civil Rights (OCR) for all HIPAA complaints, investigations, and related matters.

b. University Information Security Officer: The Information Security Officer is the University's HIPAA Security Officer. The Information Security Officer is responsible for ensuring compliance with the Security and Breach Notification Rules established at 45 CFR Parts 162 164, Subparts C and D. The University Information Security Officer will work with the University HIPAA Privacy Officer to develop, implement, and maintain policies and procedures necessary for Health Care Components 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 University Information Security Officer will coordinate with the University HIPAA Privacy Officer to monitor compliance with this Policy. The University Information Security Officer may receive, investigate, recommend resolution, and respond to possible breaches of the Security Rule. The University Information Security Office must coordinate with the University HIPAA Privacy Officer in all such actions.

2. **Designation of Health Care Components:** The University HIPAA Privacy Officer will:
    i. Establish criteria consistent with HIPAA regulations to determine those University programs that should be designated as Health Care Components;
    ii. Review, on a schedule to be established by the HIPAA Privacy Officer and otherwise as needed, University programs to properly designate Health Care Components;
    iii. Make proper Health Care Component designations in a timely manner; and
    iv. Coordinate with each Health Care Component, and provide assistance as required, with respect to the Health Care Component’s development and implementation of a HIPAA Compliance Program, as more fully described below.
3. **HIPAA Compliance Programs for Health Care Components:** The University HIPAA Privacy Officer, in conjunction with the University Information Security Officer, will coordinate with and assist the Health Care Components with the development and implementation of a HIPAA Compliance Program that is appropriate to each Health Care Component’s operations. The Compliance Program will include procedures consistent with this Policy, training, the conduct of audits and investigations, and the implementation of reasonable and appropriate corrective action plans in the event of a breach or other violation of HIPAA or this Policy. The University HIPAA Privacy Officer will conduct compliance reviews and investigations in coordination with Health Care Components and will consult with the University Information Security Officer, the University Office of General Counsel and/or other members of the

University community as necessary.

4. **Banner–University Medical Group Coordination:** The University HIPAA Privacy Officer may coordinate activities related to research and services which involve the University and Banner–University Medicine Division, including Banner–University Medical Group, Banner–University Medical Center Phoenix Campus, Banner–University Medical Center Tucson Campus, and Banner–University Medical Center South Campus. The University HIPAA Privacy Officer may assist both organizations with HIPAA-related compliance issues that impact both organizations, including training of Workforce members and investigations of violations of this Policy, uses and disclosures of PHI for research purposes, and any other standards that involve both covered research studies and UA departments, clinics, and individuals that serve as Business Associates of Banner Health Medical Centers.
5. **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 University Campus Health Service or other campus clinics, programs, or centers.

C. Policy Review

This Policy will be reviewed periodically by the University HIPAA Privacy Officer to ensure compliance with applicable laws and standards. This content of this policy will be modified as necessary or appropriate.

Related Information*

For more information on student privacy under FERPA, see www.registrar.arizona.edu/privacyguidelines.htm [2]

Code of Federal Regulations (CFR) 45 Parts 160, 162 and 164 [3]

Revision History*

Revised March 3, 2016

Revised March 24, 2015

Replaces HIPAA Privacy and Security Policy, effective March 16, 2011.

Links
[1] mailto:privacyoffice@email.arizona.edu
[2] http://www.registrar.arizona.edu/privacyguidelines.htm
[3] http://www.gpo.gov/fdsys/search/pagedetails.action?collectionCode=CFR&searchPath=Title+45%2FSubtitle+A%2FSubchapter+C&granuleId=&packageId=CFR-2007-title45-vol1&oldPath=Title+45%2FSubtitle+A%2FSubchapter+C&fromPageDetails=true&collapse=true&ycord=0